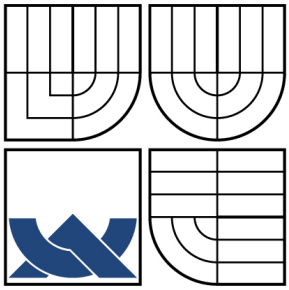
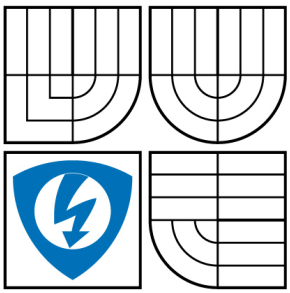


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

SOFTWAROVÁ PODPORA NÁVRHU ELEKTRONICKÉHO ZABEZPEČOVACÍHO SYSTÉMU

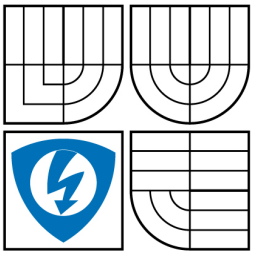
SOFTWARE DESIGN SUPPORT OF BURGLAR ALARM SYSTEM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. MICHAL VYMAZAL
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. KAREL BURDA, CSc.
SUPERVISOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Michal Vymazal	***ID:***	83130
Ročník:	2	***Akademický rok:***	2008/2009

NÁZEV TÉMATU:

Softwarová podpora návrhu elektronického zabezpečovacího systému

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte a popište problematiku návrhu elektronických zabezpečovacích systémů (EZS). Na tomto základě navrhněte vhodnou metodiku návrhu EZS pro objekty stupně zabezpečení 1 a 2. Pro praktické využití navržené metodiky zrealizujte softwarovou podporu, která by byla založena na webových technologiích. Požaduje se intuitivní grafické a interaktivní rozhraní, která umožní vytvořit kvalitní návrh EZS systému i laikům.

DOPORUČENÁ LITERATURA:

[1] ČSN EN 50131-1. Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky. ČNI, Praha 2007.
[2] Křeček, S. a kol.: Příručka zabezpečovací techniky. Blatenská tiskárna, Blatná 2003.

Termín zadání:	9.2.2009	***Termín odevzdání:***	26.5.2009

Vedoucí práce: doc. Ing. Karel Burda, CSc.

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Tato diplomová práce se věnuje realizaci softwarové podpory návrhu elektronického zabezpečovacího systému EZS pro stupně zabezpečení 1 a 2 založené na webových technologiích. Bylo vytvořeno intuitivní grafické a interaktivní rozhraní, které umožní vytvořit kvalitní návrh EZS i laikům. Nejdříve jsou v práci popsány normy a legislativy v České republice, podle kterých se návrh EZS musí řídit. V teoretické části jsou podrobně popsány vlastnosti EZS a jeho komponent, princip správného fungování, zásady instalace, výhody a nevýhody použití, jednotlivé kroky návrhu EZS a navržená metodika návrhu pro stupeň zabezpečení 1 a 2. V praktické části jsou popsány použité technologie pro realizaci práce, struktura vytvořené webové stránky a jednotlivé kroky praktického návrhu EZS, tak jak je uvidí uživatel při vytváření.

Výsledkem práce je webová stránka, která je rozdělena na dvě části: teoretickou a praktickou. V teoretické části jsou uvedeny všeobecné informace o architektuře EZS, návrhu EZS a vytvořené metodice pro návrh EZS pro stupeň zabezpečení 1 a 2. V praktické části si uživatel na základě získaných informací a za pomocí nápovědy vytvoří kvalitní návrh EZS tak, aby splňoval všechny podmínky pro spolehlivé fungování v provozu.

KLÍČOVÁ SLOVA

návrh elektronického zabezpečovacího systému, webové technologie, Drupal, MySQL, PHP, grafické rozhraní, Flash

ABSTRACT

This thesis deals with implementation of software support of alarm system design for security levels 1 and 2 based on web technologies. It was created intuitive and interactive graphical interface that allows to create high-quality alarm system design even for laymen. First of all the paper deals with standards and jurisdictions in the Czech Republic, according to which the alarm system design must be followed. In theoretical part there are described in detail characteristics of alarm systems and its components, proper functioning principles, installation principle, advantages and disadvantages of use, individual steps of alarm system design and proposed methodology of alarm system design for security level 1 and 2. In practical part there are described the technologies used for the implementation of this paper, structure of created webpage and detailed steps of alarm system design, as seen by user during creating.

The result of this paper is a webpage, which is divided into two parts: theoretical and practical. The theoretical part provides information about the alarm system architecture, alarm system design and established methodology for the alarm system design for security level 1 and 2. In the practical part the user, on the basis of gained information and interactive help, can create high-quality alarm system design that meets all the conditions for reliable function in real traffic.

KEYWORDS

alarm system design, web technology, Drupal, MySQL, PHP, graphical interface, Flash

VYMAZAL, M. *Softwarová podpora návrhu elektronického zabezpečovacího systému.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 66 s. Vedoucí diplomové práce doc. Ing. Karel Burda, CSc.

Prohlášení o původnosti práce

Prohlašuji, že svou diplomovou práci na téma „Softwarová podpora návrhu elektronického zabezpečovacího systému“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.
Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne . . . .

podpis autora

Poděkování

Děkuji vedoucímu diplomové práce doc. Ing. Karlu Burdovi, CSc. za velmi užitečnou metodickou pomoc, cenné rady při zpracování diplomové práce a její odbornou konzultaci.

V Brně dne . . . . . .

. . . . . .

podpis autora

OBSAH

SEZNAM OBRÁZKŮ A TABULEK

ÚVOD

V dnešní době se zvyšujícím se růstem kriminality je stále více kladen důraz na bezpečnost a to nejen z hlediska možné krádeže aktiv (vše, co je majitelem považováno za cenné) či vyzrazení tajemství, ale především ochranu vlastního zdraví. Zloději jsou totiž schopni i fyzického napadení, například za účelem vydírání. Celá záležitost elektronického zabezpečovacího systému ovšem není složitá, což si ale v dnešní době hodně lidí stále myslí. Jde jen o to, co nejefektivněji systém navrhnout tak, aby zákazník za rozumnou cenu získal maximální bezpečí. Zabezpečovací systém nezabrání vstupu nepovolané osoby do střeženého objektu, ale spolehlivě informuje o jeho narušení a tím minimalizuje možné hmotné škody.

Elektronický zabezpečovací systém je zařízení, jehož přítomnost nás již nepřekvapí v kancelářích, obchodech, autech, ani běžných domácnostech. Není to ale spotřební zboží, které bychom našli na pultech obchodních domů. Málokterý neodborník, který teprve uvažuje o jeho pořízení, má ucelenější představu o tom, co všechno mu může takové zařízení přinést a co od něj naopak čekat nemůže.

Cílem této práce je prostudování a seznámení se s problematikou elektronických zabezpečovacích systémů (dále jen EZS) a problematikou jejich návrhu, s čímž souvisí také seznámení se s funkcemi, vlastnostmi a zásadami použití jednotlivých komponent systému EZS. Dále ze získaných informací navrhnout vhodnou metodiku návrhu EZS pro stupeň zabezpečení 1 a 2 a pro její praktické využití realizovat programové řešení založené na webových technologiích s interaktivním a intuitivním grafickým rozhraní, které umožní vytvořit kvalitní návrh i laikům.

Práce se skládá ze čtyř kapitol. V první kapitole se hovoří o normách a legislativách používaných pro EZS v České Republice, podle kterých se návrh EZS musí řídit. Ve druhé kapitole jsou detailně popsány funkce, principy a podmínky instalace a používání jednotlivých komponent EZS. Třetí kapitola je rozdělena na dvě části. První část se věnuje obecnému návrhu systému EZS pro všechny stupně zabezpečení a jednotlivým krokům návrhu, druhá část vychází z teorie části první a popisuje vytvořenou metodiku návrhu EZS pro stupeň zabezpečení 1 a 2. V poslední kapitole je popsáno vytvořené programové řešení založené na webových technologiích.

1. NORMY A LEGISLATIVY

Diplomová práce vychází z normy ČSN EN 50131-1, jejíž nejaktuálnější změna byla vydána v roce 2007.

Norma [1], [4], [5] je určena jako pomůcka pro uživatele, pojišťovací společnosti, projektanty, dodavatele EZS a policii při stanovování kompletní a přesné specifikace ochrany pro konkrétní objekty. Norma neurčuje druh zabezpečovacího systému, rozsah či míru detekce a ani nutně nepokrývá všechny požadavky na konkrétní zabezpečovací systém.

Všechny požadavky této normy na EZS se týkají pouze základních minimálních požadavků a je nutné vzít v úvahu povahu a vlastnosti objektů, hodnotu majetku uvnitř objektů, míru rizika vniknutí případného narušitele, vlastnosti okolních staveb a další faktory, které mohou ovlivnit výběr stupně a složení zabezpečovacího systému. Aby byla zajištěna úroveň požadovaného zabezpečení, elektrické zabezpečovací systémy a jeho komponenty jsou rozděleny do čtyř stupňů zabezpečení, kde stupeň zabezpečení 4 je stupeň s nejvyšší mírou rizika, které berou v úvahu míru rizika, která závisí na typu objektu, hodnotě majetku a na předpokládaném typu narušitele.

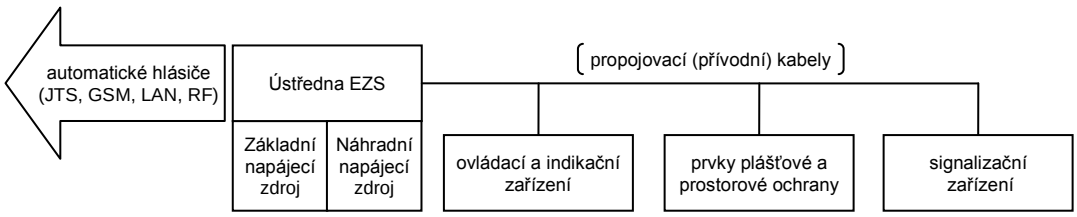
Tato norma specifikuje požadavky na provedení nainstalovaných zabezpečovacích systémů, ovšem neobsahuje požadavky pro návrh, projekci, instalaci, provoz a údržbu. Toto řeší až změna Z1 ČSN EN 50131-1. V této normě jsou specifikovány všechny požadavky pro komponenty elektrických zabezpečovacích systémů příslušné klasifikace prostředí. Tato klasifikace popisuje prostředí, ve kterém se předpokládá, že bude komponent EZS pracovat.

Pro obor zabezpečení byla zřízena Technická normalizační komise č. 124 pod názvem „Elektrická požární a zabezpečovací signalizace“, jejímž cílem je vytvoření optimální soustavy českých norem harmonizovaných s obdobnými mezinárodními a evropskými normami.

2. ELEKTRONICKÉ ZABEZPEČOVACÍ SYSTÉMY

2.1 Architektura systému EZS

Elektronický zabezpečovací systém [2] je soubor ústředen, čidel, ovládacích a indikačních zařízení, tísňových hlásičů, prostředků poplachové signalizace a přenosových zařízení, jejichž prostřednictvím je opticky nebo akusticky signalizováno na určeném místě narušení střeženého objektu nebo prostoru. Na *Obrázku 2.1* je znázorněna struktura systému EZS.



Obrázek 2.1: Zjednodušená struktura systému EZS

2.2 Ústředny EZS

Ústředna EZS [2], [5], [6] je srdcem každého zabezpečovacího systému. Je to zařízení určené k příjmu a vyhodnocení výstupních elektrických signálů čidel nebo tísňových hlásičů a k vytvoření signálu o narušení.

Ústředna EZS je zařízení, které má tyto funkce:

- Přijímá a vyhodnocuje elektrické signály z čidel,
- Ovládá zařízení, která indikují narušení (signalizační, přenosová aj.),
- Zajišťuje napájení čidel a prvků EZS elektrickou energií,
- Pomocí ovládacích zařízení umožňuje nastavení a řízení systému (uvedení do stavu střežení a do stavu klidu),
- Umožňuje diagnostiku EZS.

Požadavky zabezpečení ústředny:

- Umístění uvnitř střeženého prostoru,
- Umístění na nejkratší trase od vstupu do objektu,
- Umístění do prostoru s nejvyšším stupněm zabezpečení,
- Zamezit možnosti sledování obsluhy ústředny,
- Vyloučit přístup veřejnosti.

Kritéria výběru ústředny EZS:

- Požadovaný stupeň zabezpečení, do kterého objekt spadá (na základě bezpečnostního posouzení a následné analýzy rizik),
- Fyzický rozsah objektu, jež má být střežen, a jeho stavební provedení,
- Možnosti a požadavky zákazníka.

Rozdělení ústředen EZS
Ústředny jde podle způsobu propojení s detektory rozdělit do dvou skupin:

- *Kabelové* (nejčastěji metalické vícevodičové kabely),
- *Rádiové* (zpravidla pásmo 433MHz),
- *Hybridní* (kombinace drátového a bezdrátového připojení čidel).

2.2.1 Kabelové ústředny

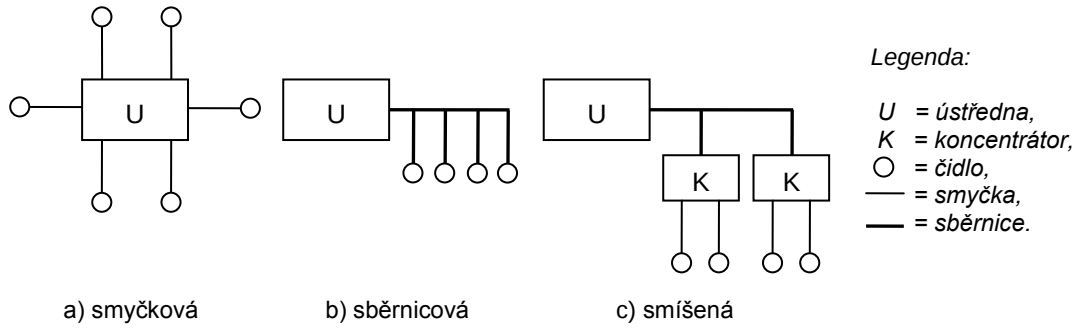
Kabelové ústředny jsou propojeny se svými komponenty pomocí kabelů.

Vlastnosti kabelových ústředen:

- Výhody
  - Nízká cena,
  - Vysoká spolehlivost.
- Nevýhody
  - Nízká variabilita rozmístění čidel.

Rozdělení kabelových ústředen (podle připojení a komunikace s detektory):

a) Smyčková,
b) Sběrnicová,
c) Smíšená.



Obrázek 2.2: Typy ústředen [6]

a) Smyčkové (analogové) ústředny

Tento typ ústředny má vstupní vyhodnocovací obvod pro každou poplachovou smyčku. Každá smyčka je zakončena zakončovacím obvodem tak, aby vykazovala předepsanou hodnotu odporu. Klidový stav je indikován sepnutým kontaktem. Změna odporu smyčky (aktivace čidla, sabotáž) vede k vyhlášení poplachu.
Kabelová síť je rozsáhlá, neboť ke každému čidlu musí být přiveden kabel příslušné smyčky. Kabel musí obsahovat dva vodiče pro napájení čidla, dva pro poplachový kontakt, dva vodiče pro sabotážní kontakt a další vodiče dodatkových funkcí.

Typy připojení čidel k ústředně (podle rozlišení detekce poplachu od sabotáže):

- Jednoduché vyvážení (nelze rozlišit),
- Dvojité vyvážení (lze rozlišit).

Jednoduché vyvážení

Pro zapojení jednoho detektoru je nutno využít 2 smyčky, jednu pro ochranu proti otevření ochranného krytu čidla (tamper) a druhou k vyhlášení poplachového stavu vyvolaného spínacím kontaktem detektoru (alarm). Smyčka umožňuje pouze detekci poplachu nebo pouze detekci sabotáže. Při tomto způsobu zapojení je potřeba dvou smyček na jeden detektor. Pro propojení je potřeba šest vodičů.

Rezistory svorkovnice čidla musí být umístěny uvnitř krabice s ochranným kontaktem. Jedině tak se zabrání možnému *přemostění* (vyřazení detektoru z funkce). V praxi se častěji využívá možnost připojení více čidel na jednu smyčku. Při tomto zapojení ovšem není možné určit, na kterém čidle došlo k otevření spínacího kontaktu. V tomto případě je nutné pro ochranný a poplachový kontakt umístit rezistor R1 do krabice nejvzdálenějšího detektoru, aby se znemožnilo přemostění.

Dvojité vyvážení

Nevýhody jednoduchého vyvážení lze částečně odstranit připojením detektorů k ústředně *dvojitým vyvážením* tak, že pro rozlišení poplachu od sabotáže se pro jedno čidlo použije pouze jedna smyčka, která se někdy využívá i k napájení některých čidel. Při dvojitém vyvážení je možné zapojit více čidel na jednu smyčku.

Vlastnosti smyčkových ústředen:

Výhody

- Velmi jednoduchý,
- Velmi spolehlivý.

Nevýhody

- Velké množství kabeláže,
- Omezené množství smyček.

b) Sběrnicové ústředny

Sběrnicová ústředna, také nazývána jako ústředna s *přímou adresací čidel*, pracuje na principu komunikace po datové sběrnici ústředna – čidla a komunikační protokol je typu dotaz – odpověď (dotazy vysílá ústředna a odpovědi zasílají čidla). Ústředna periodicky generuje adresy čidel a přijímá jejich odezvy. Každé čidlo je opatřeno komunikačním modulem (chip – ID bod).

Kabelová síť je minimální, neboť je tvořena téměř libovolnou konfigurací, omezená specifikacemi výrobců (maximální délka sběrnice, maximální počet odboček z páteřního paprsku, maximální počet čidel na sběrnici). Je tvořena čtyřvodičovým vedením, kde dva vodiče slouží pro napájení čidla a dva jako drátová sběrnice.

Čidla jsou na sběrnici připojena v libovolném pořadí. Každé čidlo má svou unikátní adresu, aby nedocházelo ke kolizím. Při narušení objektu tedy ústředna oznámí, které

konkrétní čidlo bylo aktivované a jaký je druh narušení (poplach, sabotáž, případně další stavy). Zpravidla se používá standard RS 485 (přenosová rychlost jsou desítky kb/s, dosah několik stovek metrů, dobrá odolnost vůči poruchám a rušení).

Vlastnosti sběrnicových ústředen:
Výhody

- Jednoduchá kabeláž,
- Minimální délka vedení,
- Přesná identifikace čidla a události jím vyvolané.

Nevýhody

- Nelze realizovat dodatkové funkce čidel,
- Dražší a komplikovanější čidla,
- Systém často náchylné na elektromagnetické rušení a elektrické vedení,
- Citlivost (plané poplachy),
- Vliv úbytku napětí na dvojici vodičů k napájení na chod systému.

Kompromis

- Omezený počet čidel (kompromis mezi požadavkem na rychlou odezvu systému a nízkou přenosovou rychlost na sběrnici).

c) Smíšené ústředny

Jedná se o kombinaci smyčkové a sběrnicové ústředny. Jde tedy o dobrý kompromis z hlediska složitosti kabeláže a nákladů na systém. Na společnou sběrnici ústředny jsou připojeny tzv. koncentrátory. Koncentrátory komunikují s ústřednou stejně podobně jako čidla u sběrnicové ústředny. Na koncentrátory jsou čidla připojena pomocí smyček. Každý koncentrátor nepřetržitě monitoruje svá čidla a současně ústředna periodicky zasílá výzvy jednotlivým koncentrátorům. Vlastní vyhodnocování probíhá podle typu ústředny různě.
Pokud je kapacita ústředny dostatečná, je možné na jednotlivé vstupy koncentrátorů připojit přímo jednotlivá čidla. Tím přejde typ ústředny na ústřednu s přímou adresací čidel a jejími výhodami. Omezujícím faktorem však budou vysoké náklady. Je potřebné navrhnout optimální rozdělení čidel do smyček tak, aby byla zachována účelná úroveň adresace. Tento typ umožňuje realizaci dodatkových funkcí přímo přes sběrnici.

2.2.2 Rádiové (bezdrátové) ústředny

Rádiové ústředny jsou sběrnicového typu. Sběrnice je rádiová, většinou v pásmu 433 MHz. Dosah sběrnice ve volném prostranství je v závislosti na použitém systému v řádech stovek metrů (100 – cca 1000 m). Uvnitř objektů klesá tato vzdálenost přibližně na desítky metrů (10 – 100 m).
Čidla jsou napájena buď lithiovou baterií, nebo 9V destičkovým článkem. Napětí baterie je hlídáno a při poklesu na určitou hladinu tuto skutečnost sdělí čidlo ústředně při své nejbližší odpovědi.

Přenos dat je u současných bezdrátových systémů *duplexní* a každý prvek systému je vybaven jak vysílací, tak přijímací elektronikou – modulem vysílač/přijímač. Tyto moduly jsou schopny si ve vyhrazeném kmitočtovém pásmu najít dva volné kanály pro přenos a automaticky se na ně naladit.

Výhody duplexní komunikace (oproti starší poloduplexní komunikaci):

- Při zapínání systému je ústřednou ověřen stav všech prvků,
- Čidla v klidovém stavu nevysílají (neplýtvají energií), nemusí být vybavena blokováním dalšího vysílání po vyslaném poplachu,
- Ověření ústřednou, zda je poplachová informace skutečný poplach (minimalizace planých poplachů).

Zabezpečení rádiových ústředen:

- *Kmitočtová adaptace* – umožňuje automatické vyhledávání a naladění nerušeného kanálu (ochrana před záměrným i neúmyslným rušením),
- *Plovoucí kód* – časově proměnný kód, který slouží prvkům EZS k autentizaci předávaných dat.

Kódování přenosu a prvků

Mezi ústřednou a ostatními prvky bezdrátových systémů dochází ke kódování komunikace (poplach, ověření poplachu, porucha zdroje, test, slabá baterie prvků aj.). Jednotlivé prvky je nutné identifikovat. To lze provést naprogramováním mechanickými přepínači binárním způsobem nebo pomocí připojeného počítače. U moderních systémů mají prvky kód pevně přidělen při výrobě. Jejich čísla se programují do ústředny při instalaci systému. Tím je znesnadněno cílené nahrazení prvku s konkrétní adresou při pokusu o nabourání systému.

Vlastnosti bezdrátových ústředen:

Výhody bezdrátových systémů vyplývají z absence kabelového vedení:

- Snadná instalace,
- Minimalizace kabelové sítě,
- Instalace do hotových objektů s minimálním zásahem,
- Snadné rozšíření systému, popř. změna rozmístění prvků.

Nevýhody:

- Snížení bezpečnosti a spolehlivosti,
- Absence ochrany proti sabotáži (narušení provozního pásma),
- Poruchovost způsobena vlivem rušení jiných zařízení (je-li provozovatelem fyzická osoba, je obtížné zařízení vypátrat a přimět k zastavení provozu),
- Stále dražší než kabelové systémy.

Bezdrátové systémy je vhodné instalovat pouze v prostorách, které vylučují možnost použití kabelových rozvodů. Hlavním důvodem je nižší spolehlivost.

2.2.3 Hybridní ústředny

Hybridní rozvody zabezpečovacích systémů jsou jakousi snahou vytěžit z obou hlavních směrů datových rozvodů EZS to nejlepší a minimalizovat naopak jejich nedostatky. Většina současných moderních ústředen je hybridní, tedy umožňuje jak připojení drátových snímačů (zón), tak i případné bezdrátové připojení, pomocí rozšiřujících bezdrátových modulů.

2.2.4 Obvody ústředen

Obvody ústředen EZS [1], [2] se dělí na tři skupiny:

- Vstupní vyhodnocovací obvody
- Výstupní obvody ústředen
- Napájecí obvody

a) Vstupní vyhodnocovací obvody

Jednotlivá čidla EZS jsou připojena do poplachové nebo tísňové a sabotážní smyčky. Elektrické parametry všech druhů smyček jsou shodné, liší se pouze způsobem hlášení svého narušení. Typ ústředny udává počet vstupů smyček, který se může pohybovat od čtyř až po stovky.
U nejjednodušších ústředen bývají vstupní obvody obvykle velmi primitivní a jsou schopny vyhodnotit pouze dva základní stavy: smyčka uzavřená, smyčka otevřená. Správný stav se volí „smyčka uzavřená“, neboť každý destrukční zásah do čidla nebo kabeláže vede k poplachovému stavu „smyčka rozpojená“.
U ústředen vyššího standardu jsou tyto obvody dokonalejší a pracují jako přesné odporové děliče nebo jako vyvážené měřící můstky.

b) Výstupní obvody

Tyto obvody umožňují aktivovat výstupní signalizační a indikační obvody a prvky systému EZS. Tyto výstupy jsou použity pro prvky EZS, jako např.:

- *Akustická signalizace (siréna)* – výstup bývá programovatelný, umožňuje volit dobu funkce, dobu zpoždění, přerušování zvuku sirény,
- *Optická signalizace (zábleskový maják)* – obvod se obvykle spíná současně s výstupem pro akustickou signalizaci, zůstává aktivní i po jejím doznění až do vynulování ústředny, občas bývá programovatelný,
- *Programovatelné výstupy* – umožňují vytvořit potřebné výstupní signály pro různé periferie (inteligentní sirény, přenosy pro diagnostiku EZS atd.),
- *Výstupy pro periferie* – k dispozici u ústředen vyšší kategorie, jsou to především výstupní porty pro napojení registračních zařízení, signalizační tablo, sériové přenosové kanály pro připojení PC nebo programovacích modulů,
- *Bezpotenciálové vstupy* – pomocí těchto výstupů lze vytvářet atypické funkční vazby mezi EZS a dalšími doplňkovými bezpečnostními systémy

(uzavřené televizní okruhy CCTV, systémy kontroly, systém aktivace osvětlení objektu poplachovým signálem aj.).

c) Napájecí obvody

Napájecí obvody slouží k napájení elektronických obvodů ústředny a všech návazných komponent systému EZS.

Ústředna obsahuje vždy dva zdroje:

- *Základní napájecí zdroj* – zdroj elektrické energie pro trvalé napájení všech zařízení EZS, musí být schopen dodat potřebný proud, který je součtem proudových odběrů všech prvků systému EZS včetně ústředny připojených na daný zdroj, musí být dimenzovaný tak, aby po skončení nejdelšího výpadku sítě byl schopen dodat proud pro všechny připojené prvky a proud potřebný k dobíjení akumulátorů během doby stanovené normou,
- *Náhradní napájecí zdroj* – zdroj elektrické energie pro napájení všech zařízení EZS při výpadku základního zdroje, je tvořen bezúdržbovými olověnými akumulátory, musí být dimenzován tak, aby byl schopný překlenout nejdelší výpadek základního napájecího zdroje dle normy.

Pro napájecí zdroj platí tato pravidla:

- Musí být připojen k síti uvnitř střežených objektů,
- Musí být použit výhradně jen pro EZS,
- Musí mít odpovídající větrání,
- Nesmí být instalován v místech, kam má přístup veřejnost,
- Musí být instalován uvnitř střežených objektů,
- Umístění musí umožňovat snadnou obsluhu,
- Nesmí být instalován na obvodovou stěnu, pokud nemá pevnou konstrukci,
- Napájení pro EZS musí být přiváděno přes:
  - pojistkou jištěné místo,
  - nevypínanou zásuvku.

2.3 Čidla

Čidlo EZS [2], [4], [5] je zařízení, které reaguje na jevy související s narušením střeženého objektu nebo prostoru nebo s nežádoucí manipulací se střeženým předmětem vytvořením předem určeném výstupního elektrického signálu.

Obecné zásady při výběru čidel:

- V detekčním rozsahu čidla nesmí být pohyblivé předměty,
- Správně zvolit čidla pro dané klimatické podmínky,
- Provádět montáž v souladu s pokyny výrobce,
- Vybírat čidla s potřebným pokrytím střeženého prostoru s požadavky na individuální identifikaci elektronických čidel v případě jejich aktivace,

- Možnost kontroly činnosti čidel,
- Umístění odrazující od jejich demontáže nebo narušení.

2.3.1 Prvky plášťové ochrany

Slouží k hlídání otevření nebo destrukci prostupů pláště budovy (okna, vrata, dveře).

a) Magnetické kontakty (čidla otevření)

Magnetické kontakty jsou vždy tvořeny dvojicí dílů:

- *Permanentní magnet* – nejčastěji je použit zmagnetovaný váleček z feritu
- *Jazýčkový kontakt* – tvořen zatavenou trubičkou naplněnou ochrannou atmosférou, v níž jsou umístěny dva feromagnetické kontakty

V klidovém stavu je kontakt jazýčkového relé sepnut magnetickým polem permanentního magnetu. Oddálením magnetu se kontakt rozepne a způsobí vyhlášení poplachu. Obě části jsou samostatně zapouzdřeny do krytů z nemagnetického materiálu (plast, hliníková slitina). Na rám střeženého otvoru se instaluje jazýčkový kontakt, na pohyblivou část se instaluje permanentní magnet.

Vlastnosti magnetických kontaktů:

- Různé provedení umožňuje povrchovou nebo skrytou montáž přímo do dveří či oken,
- Pro speciální aplikace s velmi vysokými riziky (věznice aj.) existují kontakty odolné proti cizímu magnetickému poli,
- Pro střežení prostupů s roletami je použit magnetický kontakt v těžkém, mechanicky i klimaticky odolném provedení (vodotěsné),
- Jakýkoli pokus o sabotáž (přiložení cizího magnetu) vyvolá automaticky poplach.

Zásady instalace magnetických kontaktů:

- Dodržovat stanovené maximální a minimální vzdálenosti magnetu od jazýčkového kontaktu v klidové poloze,
- Umístit tak, aby bylo detekováno otevření dveří či oken při oddálení max. 30 mm, u vrat a bran na principu křídel či posuvu jejich částí max. 50 mm,
- Umístit tak, aby bylo detekováno odejmutí předmětů,
- Umístit tak, aby při běžném pohybu částí nedošlo k aktivaci (drnčení),
- Instalovat pouze uvnitř střežených objektů,
- Posoudit potřebný rozsah otevření pro vstup nebo odejmutí předmětů a podle těchto údajů umístit spínače (prostrčení ruky),
- Dodržovat orientaci a polohu magnetu (stanoví-li výrobce)
- Používat zásadně šrouby z nemagnetického materiálu,
- Pro montáž na magnetický materiál použít výrobcem povolené kontakty,
- Osazovat všechny pohyblivé části prostupů (obě pohyblivá křídla),
- Jazýčkový kontakt instalovat vždy na stranu křídla proti pantům,

- Přívodní vodič musí být veden skrytě (v elektroinstalačních trubkách či lištách) přímo do propojovací krabice,
- Neprovádět nechráněná propojení vodičů pod bužírkou,
- Neinstalovat v místech, kde může být spínač úmyslně aktivován.

Příčiny planých poplachů:

- Nedodržení pokynů výrobce při montáži,
- Omylem nezajištěné prostupy (okna, dveře),
- Špatně doléhající okna a dveře.

Rozdělení magnetických kontaktů podle použití:

- Kontakty pro povrchovou montáž,
- Závrtné kontakty,
- Odolné kontakty (vrata).

Obrázek 2.3: Povrchový kontakt [3]

Obrázek 2.4: Závrtný kontakt [3]

Obrázek 2.5: Masivní vratový kontakt [3]

b) Detektory tříštění skla (GBS)

GBS (Glass Break Sensor) detektory fungují na principu vyhodnocování akustického efektu při tříštění skla. Elektronika čidla vyhodnocuje akustické vlnění přijaté elektretovým mikrofonem. Pásmová propust čidla propustí jen část spektra typickou pro tříštění skla. Více pásmových propustí umožní vyhodnocení přítomnosti zvuku ve více částech zvukového spektra, tím dochází k minimalizaci falešných poplachů. Nejnovější typy vyhodnocují zvukové spektrum ve více diskrétních bodech a poplachové hlášení je vyvolané tehdy, jsou-li všechny tyto kmitočty ve zvuku v určitém intervalu obsaženy.

Zásady instalace akustických čidel rozbití skleněných ploch:

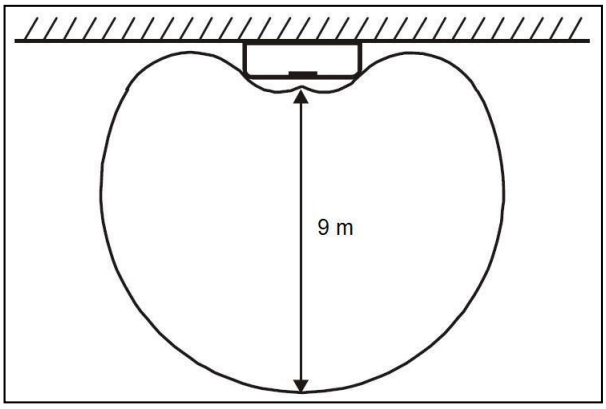
- Montovat proti chráněným plochám,
- Zachovat mezi čidlem a střeženou plochou volný prostor(nepoužívat závěsy),
- Dbát instrukcí výrobce ohledně směrování snímacího prvku čidla a jeho garantovaného dosahu s ohledem na provedení skleněné plochy (různé tloušťky a provedení – sklo lepené, kalené, laminované, drátové…),
- Vyvarovat se přítomnosti akustických zdrojů (mechanické zvonky),
- Izolovat střežený prostor od venkovních akustických zdrojů,

- Dodržet detekční prostor,
- Brát v potaz přítomnost podlahovin a obkladů stěn a jejich vliv na účinnost čidla (akusticky odrážející krytiny mají tendenci zvyšovat rozsah/citlivost),
- Zohlednit snížení citlivosti čidla při použití záclon či žaluzií,

Příčiny planých poplachů:

- Silný opravní provoz se skřípavými zvuky tramvají, vlaků či brzd autobusů,
- Přítomnost zvěře v objektu (ptáci, hlodavci, hmyz),
- Přítomnost kontejnerů na sklo v blízkosti detektoru,
- Technické vybavení prostor (telefony, zvonky, faxy),
- Vliv podlahovin a obkladů stěn na účinnost čidla (odrážející krytiny),
- Přítomnost předmětů vydávající zvuky s obdobným charakterem jako rozbíjení skla (řinčící předměty).

Snímací prostorová charakteristika detektoru GBS je zobrazena na *Obrázku 2.6*.



Obrázek 2.6: Prostorová charakteristika detektoru GBS [3]

2.3.2 Prvky prostorové ochrany (čidla prostorová)

Prostorová ochrana tvoří důležité doplnění k plášťové ochraně.

Základní dělení prostorových čidel:

a) *Čidla pasivní* – registrují fyzikální změny ve svém okolí,
b) *Čidla aktivní* – vytvářejí své pracovní prostředí aktivním působením na své okolí a detekují změnu takto vytvořeného fyzikálního prostředí.

V praxi je možné se setkat s několika druhy čidel pohybu:

- Pasivní infračervená čidla (Passive Infra Red – PIR),
- Aktivní ultrazvuková čidla (Ultrasonic – US),
- Aktivní mikrovlnná čidla (Microwave – MW),
- Duální čidla (PIR – US, PIR – MW),
- Aktivní infračervená čidla (Active Infra Red – AIR),
- Kombinovaná čidla.

Antimasking

Funkce *ochrany proti zastínění* (tzv. antimasking) je další doplňkovou funkcí, která přináší vyšší úroveň bezpečnosti. Je aktivní v době klidu objektu a slouží k indikaci zastínění čidla. Čidla s funkcí ochrany proti zastínění se aplikují v prostorech veřejně přístupných, kde je riziko sabotáže systému s cílem připravit si objekt na vloupání ve stavu střežení. Výstup této indikace je projektován na samostatnou smyčku, nebo bývá funkčně spjat s příslušnou poplachovou smyčkou, do níž je čidlo připojeno.

Důvody pro nasazení čidel s funkcí antimasking:

a) *Objekt se strážní službou* – požadavek okamžité indikace zastínění čidla či jeho přestříkání barvou.
b) *Objekt bez strážní služby* – požadavek zabránění uvedení do stavu střežení, je-li některé z čidel vybavených touto funkcí zastíněno.

a) Pasivní infračervená čidla (PIR)

PIR (Passive Infrared) čidla jsou nejčastěji používanými senzory v prostorové ochraně. Nevyzařují žádnou energii, navzájem se neovlivňují a mohou být nainstalovány tak, že se jejich detekční zóny (aktivní, neaktivní) překrývají.
Jsou založeny na principu zachycení změn vyzařování elektromagnetického záření v infračerveném pásmu kmitočtového spektra. Každé těleso, jehož teplota je vyšší než -273 °C (absolutní nula) a nižší než 560 °C, je zdrojem vyzařování vlnění v infrapásmu odpovídajícím teplotě tělesa.
Při návrhu je důležité uvážit tvar zorného pole. V závislosti na tvaru střeženého prostoru se volí čočka s odpovídajícím zorným polem. Tvar zorného pole je závislý na provedení optiky čidla, dosah čidla je závislý na kvalitě optiky, citlivosti senzoru a způsobu vyhodnocení. Správnou volbou optiky je možné střežit prostor do vzdálenosti cca 15 m či dlouhé prostory do cca 60 m. Čidly určenými pro stropní montáž lze kruhovým uspořádáním optiky obsáhnout velkou plochu v rozsahu 360°.

V praxi je možné se setkat s optikou trojího druhu:

a) *Soustava Fresnelových čoček* – nejčastější, ekonomické řešení, optický obraz skutečnosti není ideální,
b) *Soustava křivých zrcadel* – optický obraz je zobrazení skutečnosti bez kompromisu, náročnější na návrh a technologii výroby, větší dosah,
c) *Soustava černých zrcadel* – snižuje náchylnost čidel k planým poplachům vyvolaný vlivem záření o vysoké energii ve viditelném spektru (reflektory automobilů, odlesky slunce apod.).

Zásady instalace PIR čidel:

- Čidla se mají instalovat tak, aby směr pohybu pachatele byl kolmý (tangenciální) na myšlený průmět aktivní či neaktivní zóny do půdorysu střeženého objektu.
- Předpoklad spolehlivosti čidel je umístění na pevném podkladu bez vibrací.

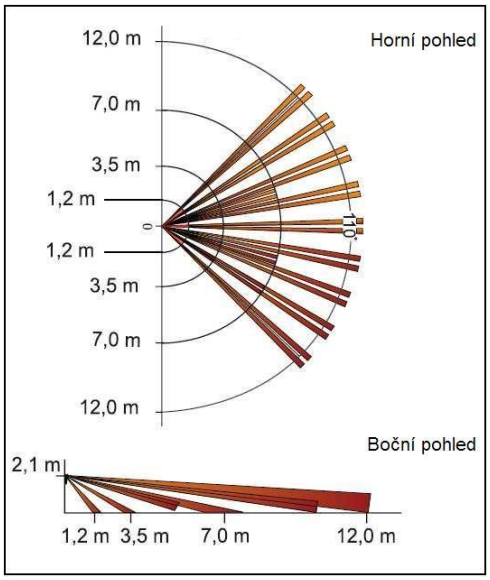
- Do jednoho prostoru je možné instalovat více PIR čidel bez nebezpečí vzájemného ovlivňování, neboť čidla nevyzařují žádnou energii.
- V případě nutnosti úplného vykrytí střeženého prostoru se doporučuje instalace více čidel k vzájemnému překrytí zón.
- Ve střeženém prostoru se nesmí nacházet tělesa prudce měnící svou teplotu.
- Od nasazení PIR čidel se upouští u prostor s podlahovým vytápěním.
- PIR čidla nesmějí být nasměrována na okna, vnější dveře a vrata kvůli možnému výskytu těles vyzařujících velké množství infračerveného záření (reflektory automobilů, odlesky slunce aj.).

PIR čidla nesmí být vystavena následujícím vlivům:

- Ventilace (vstupy a výstupy, průvan, turbulence vzduchu),
- Přímé nebo nepřímé vyzařování světla (slunce, reflektory),
- Proměnné zdroje tepla (topení, komíny),
- Spínané rušivé IR zdroje (žárovky).

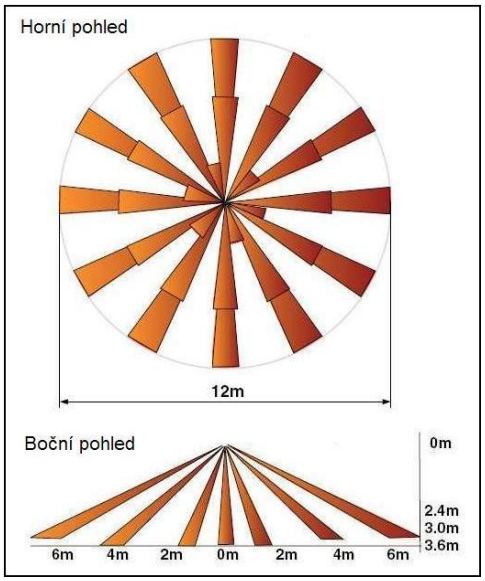
Rozdělení umístění PIR čidel dle typu zorného pole:

- a) Rohy místností



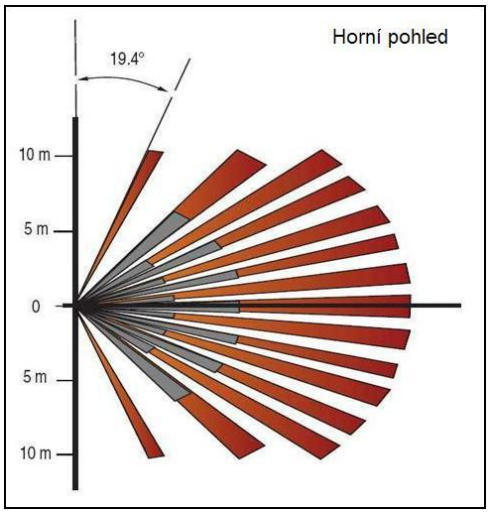
Obrázek 2.7: Standardní čočka [3]

- b) Střed stropu



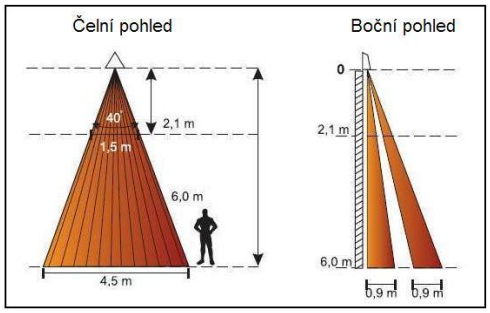
Obrázek 2.8: Kruhové uspořádání čoček (záběr 360°) [3]

- c) Střed stěny



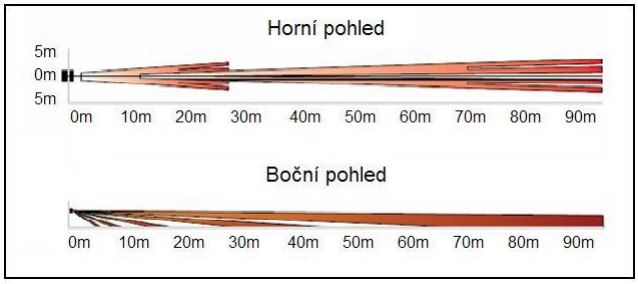
Obrázek 2.9: Čočka se širším záběrem [3]

- d) Prostor nad prostupy



Obrázek 2.10: Záclona [3]

- e) Dlouhé chodby



Obrázek 2.11: Čočka s dlouhým dosahem [3]

Zdokonalování detekce PIR detektorů [6]

Hlavními důvody je především minimalizace falešných poplachů a spolehlivější detekce narušení střeženého prostoru či pohybu v něm.

Nejčastější typy zdokonalování:

- Zvětšení šířky svazku,
- Kompaktní konstrukce čočky – zabránění vniku hmyzu a prachu do čidla,
- Inteligentní vyhodnocování informací z více zdrojů
  - *Dva svazky detektoru (horní, dolní)* – eliminace falešných poplachů vyvolaných např. domácími zvířaty (tzv. PET detektor),
  - *Dva PIR detektory v jedné chodbě* – minimalizace falešných poplachů (poplach je vyvolán, pokud pohyb zaznamenám oběma čidly).

b) Ultrazvuková čidla (US)

US (Ultrasonic sensors) čidla jsou aktivní čidla, které vyzařují do prostoru energii, jejíž odražené složky zpětně analyzují a vyhodnocují. Využívají část spektra mechanického vlnění nad pásmem kmitočtů slyšitelných lidským uchem (slyšitelné např. pro psy, komáry). Pracují na principu změny kmitočtu odraženého

ultrazvukového signálu (cca 40kHz) od pohybujícího se objektu (tzv. Dopplerův jev). Vysílač generuje konstantní signál. Přijímač přijímá vlnění odražené od překážek v prostoru. Po krátké době se v prostoru vytvoří klidový stav. V klidovém stavu je přijatá vlna stejná jako vlna vyslaná. Pohybuje-li se v prostoru libovolné těleso, způsobí změnu části kmitočtu přijaté vlny. Tato změna fáze je vyhodnocena elektronikou a je vyhlášen poplach.
Dopplerův jev lze matematicky popsat vztahem:

$$f_1 = \frac{f}{1-\left(\frac{v}{c}\right)^2} \tag{2.1}$$

kde $\boldsymbol{f_1}$ je kmitočet přijatý přijímačem,
$\boldsymbol{f}$ je kmitočet vyslaný vysílačem,
$\boldsymbol{v}$ je rychlost pohybu pohybujícího se tělesa (odrazné plochy),
$\boldsymbol{c}$ je rychlost pohybu vlnění užitého k detekci (rychlost zvuku u US čidla, rychlost pohybu elektromagnetického vlnění u MW čidla).

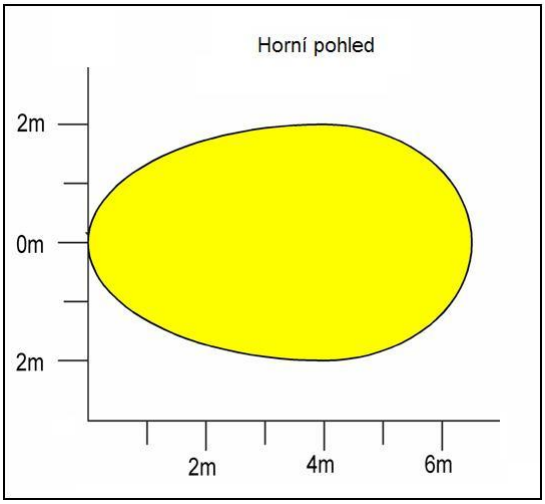
Zásady instalace US čidel:

- Čidla se mají instalovat tak, aby směr pohybu pachatele směřoval k čidlu či od něj (radiálně) – typický dosah je přibližně cca 10 m.
- Prostor musí být uzavřený, aby dosah čidla nepřesahoval mimo prostor určený ke střežení.
- V prostorech obsahujících předměty absorbující ultrazvuk (koberce, pěnové materiály) se může citlivost čidel značně změnit jejich přiblížením či oddálením. Následkem změny citlivosti čidla je snížení spolehlivosti detekce.
- Předměty umístěné do blízkosti čidel po jejich instalaci a nastavení mohou ovlivnit citlivost čidel a vést k falešným poplachům.
- Čidla nelze instalovat do prostor s často se měnícím interiérem (sklady).
- Více US čidel lze v jednom prostoru instalovat pouze tehdy, není-li možné jejich vzájemné negativní ovlivňování (mají-li různé frekvence, jsou-li vysílače synchronizovány nebo kmitočtově stálé),
- Dbát na správnou montážní výšku čidla (může ovlivnit rozsah detekce).

US čidla pohybu se nesmí instalovat:

- V prostorách s volně zavěšenými předměty (lampy),
- V prostorách s volně se pohybujícími zvířaty během střežení (hlodavci),
- Na zavěšené montážní konstrukce,
- Nad topná tělesa,
- V prostorách s teplovzdušným topením,
- V blízkosti zdrojů zvuku se širokým kmitočtovým spektrem (telefon).

Zorné pole US čidla je znázorněno na *Obrázku 2.12*.



Obrázek 2.12: Velikost pole snímané US čidlem [3]

c) Mikrovlnná čidla (MW)

MW (Micorwave sensors) čidla tvoří aktivní systémy zachycení pohybu, které jsou založeny na stejném principu jako ultrazvuková čidla (Dopplerův jev), ale místo ultrazvuku využívají elektromagnetickou energii v pásmu frekvencí 2,5GHz, 10GHz nebo 24GHz. Jsou technologicky uzpůsobeny danému kmitočtovému pásmu.
V současnosti jsou realizovány v podobě mikropáskového vedení integrovaného do desky plošných zdrojů. Oproti dřívější technologii vlnovodů je tato varianta výrazně levnější a zajistila zvýšení dostupnosti MW čidel. Díky polarizaci MW antén je možný současný provoz více detektorů v jedné oblasti bez vzájemného ovlivňování.

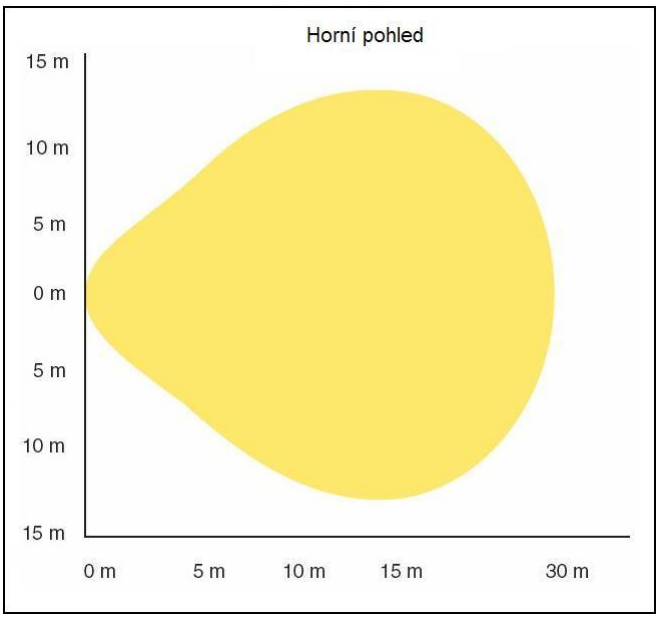
Zásady instalace MW čidel:

- Čidla instalovat tak, aby směr pohybu pachatele vedly k čidlu (radiálně),
- Čidla se musí instalovat tak, aby činnost čidla neovlivňovaly podněty mimo střežený prostor (nesmí docházet k průniku skrz stěnami objektu).

MW čidla pohybu se nesmí instalovat:

- V blízkosti velkých kovových předmětů v pásu pokrytí čidla (od objektů s rovinným povrchem se mikrovlny odrážejí a výrazně mění detekční charakteristiku, kovové potrubí),
- V blízkosti velkých kovových předmětů i mimo pásmo pokrytí,
- V blízkosti pohybující se kapaliny v potrubí z plastů,
- V prostorách, ve kterých může ve stavu střežení docházet ke spínání zářivkovitého osvětlení,
- Dochází-li k jejich vzájemnému negativnímu ovlivňování (více čidel lze v jednom prostoru použít tehdy, pracují-li na jiné vysílací frekvenci nebo jsou-li aplikovány bez možného ovlivňování).

Zorné pole MW čidla je znázorněno na *Obrázku 2.13.*



Obrázek 2.13: Velikost pole snímané MW čidlem [3]

d) Aktivní infračervená čidla (AIR)

Čidla AIR (Active Infrared) jsou další variantou infračervených čidel. Tato čidla vysílají infračervené paprsky a přijímají jejich odraz od těles ve střeženém prostoru. Aktivitu čidla je možné zjistit sledováním jeho vyzařování. Na rozdíl od ostatních aktivních čidel (ultrazvuková, mikrovlnná) mohou AIR čidla fungovat v místnostech se zapnutou klimatizací, podlahovým vytápěním nebo v místnostech s prudkými změnami teploty. AIR čidla jsou velmi přesná a jsou schopna detekovat pohyb objektu nevyzařující teplo a to i pohyb libovolně nízkou rychlostí.
Jejich velká nevýhoda je, že mají mnohem větší odběr elektrické energie oproti PIR čidlům.

e) Duální čidla

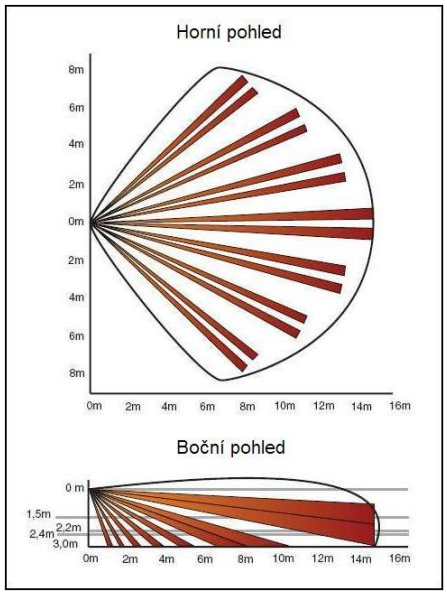
Duální čidla pracují na principu kombinace dvou funkčně odlišných typů detekce. Vývoj duálních čidel vychází z faktu, že každá technologie je jinak náchylná na plané poplachy (různá čidla fungují na různých fyzikálních principech). Kombinací různých technologií, různých fyzikálních jevů, se sníží počet špatně vyhodnocených případů. Detektor vyhlásí poplach jen v případě, dojde-li ve stanoveném intervalu k aktivaci obou senzorů.

Nejčastější kombinace duálních detektorů:

- Infračervený a mikrovlnný detektor (PIR + MW),
- Infračervený a ultrazvukový detektor (PIR + US),
- Dva infračervené detektory (PIR + PIR) s rozdělením detekovaného prostoru na dvě horizontální zóny.

Duální detektory jsou použity v případě problémových a náročných instalací, v prostorách s výrazným negativním vlivem okolí.
Pro instalaci těchto typů čidel je nutné vycházet z pravidel, která jsou platná pro jednotlivé systémy v čidlech užitých. Je třeba si uvědomit, že se práh detekce čidel díky použitému principu posunul výše oproti čidlům s jediným systémem detekce.

Zorné pole duálního PIR+MW čidla je znázorněno na *Obrázku 2.14*.

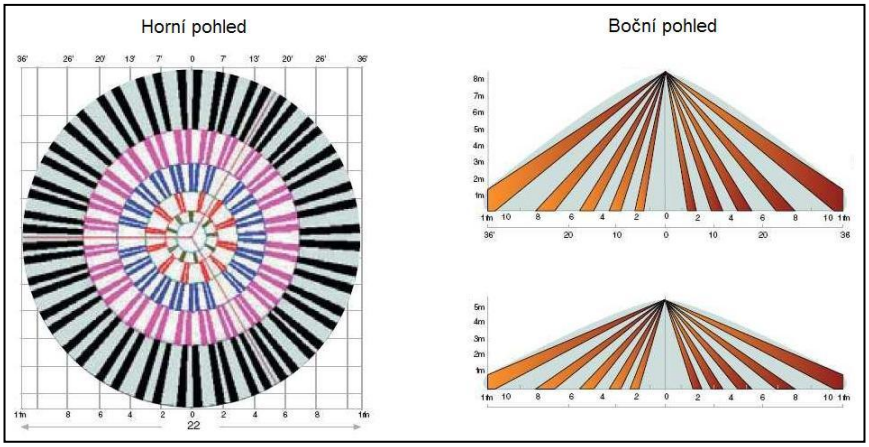


Obrázek 2.14: Duální čidlo PIR+MW [3]

f) Kombinované detektory

Oproti duálním čidlům jde u kombinovaných čidel o kombinaci dvou senzorů, které mají jiný detekční účel. Nejčastější kombinací je spojení detektoru pohybu s detektorem tříštění skla. Poplach je vyhlášen již při aktivaci jednoho čidla. To ovšem může vést k planým poplachům typickým pro jednotlivá čidla. Používá se především z ekonomických důvodů.

Zorné pole kombinovaného čidla (PIR + GBS) je znázorněno na *Obrázku 2.15*.



Obrázek 2.15: Kombinované čidlo [3]

2.4 Ovládací a indikační zařízení

Primární funkcí ovládacího zařízení [2], [4], [5] je uvedení systému EZS do stavu střežení a stavu klidu. Vhodný typ zařízení se volí podle úrovně rizik (stupně zabezpečení) a požadavků zákazníka. Cílem je jednoduchá obsluha bez zbytečných vyvolání planých poplachů při manipulaci a současně dostatečná ochrana proti překonání.

Kromě základní funkce slouží ovládací a indikační zařízení k:

- Zadávání uživatelských kódů pro ovládání systému,
- Odstavení a resetování poplachů,
- Odpínání a připínání smyček (pro částečné střežení),
- Volbě speciálních funkcí (tísňové hlášení z klávesnice, vyvolání paměti aj.),
- Programování parametrů systému.

Indikační prvky informují o provozních stavech celého systému EZS těmito způsoby:

- Opticky pomocí LED,
- Pomocí akustické signalizace,
- Kombinací akustické a optické signalizace,
- Pomocí alfanumerického displeje.

2.4.1 Klávesnice

Nezbytnou součástí každého systému je alespoň jedna klávesnice.

Rozdělení typů klávesnic:

- Klávesnice s LCD displejem,
- Klávesnice s podsvícením kláves (LED diody),

Funkce klávesnice již byly zmíněny při popisu funkcí ovládacích a indikačních zařízení. Slouží tedy především pro uvedení do stavu střežení a stavu klidu systému EZS. Při programování systému se projeví komfort, který poskytuje LCD displej. Displej je užitečný také k prohlížení historie událostí.
U klávesnic s podsvícením kláves probíhá potvrzení a zobrazení hodnot prostřednictvím podsvícení kláves, což bývá velmi nepřehledné a pomalé.
Propojení se systémem EZS je totožné, jako je tomu u rozšiřujících modulů. Často je využita společná komunikační linka. Některé klávesnice v sobě integrují vstupy a výstupy pro detektory a jiná zařízení.

Pro instalaci a používání klávesnic platí určitá pravidla:

- Elektronika klávesnice musí být v samostatné skříni,
- Klávesnice musí být umístěna uvnitř střežených prostor,
- Klávesnice musí být umístěna tak, aby neoprávněné osoby nemohly sledovat

ovládání klávesnice zařízení, není-li chráněna nebo ukryta,

- Je nutné pečlivě navrhnout přístupové a odchodové postupy s cílem minimalizovat plané poplachy,
- Je nutné zajistit potřebnou signalizaci pro účely identifikace poruch nebo poplachu.

Problémem používání klávesnice z pohledu uživatele může být nutnost zapamatování si správného kódu pro ovládání systému EZS a nutnost změny tohoto kódu. Trvalý provoz s jedním neměnným kódem může vést k vyzrazení kódu i k fyzickému opotřebení používaných tlačítek, což sníží počet možných kombinací.
Naopak mezi výhody patří možnost použití tísňového kódu v rizikovém okamžiku vstupu do objektu. Moderní typy klávesnic umožňují ovládání například osvětlení ve střežených objektech.

Pro zvýšení komfortu slouží dálkové ovladače, které mohou také spouštět garážová vrata, zavírat brány ale i pomoci předáním informace na telefon v případě tísně. U skutečně progresivně navrženého alarmu lze systém ovládat i pomocí mobilu.

2.5 Doplňková zařízení

Mezi doplňková zařízení [2], [3], [5] patří všechna samostatná zařízení, která jsou řízena řídícími výstupy a která jsou umístěna v krytu ústředny, nebo mimo ni.

2.5.1 Akustická signalizace (siréna)

Jde o nejčastěji instalované doplňkové zařízení. Používána pro vnitřní i venkovní použití. Základ tvoří akustický měnič doplněný generátorem kolísavého tónu a zesilovačem. Sirény se nejčastěji umísťují na průčelí střeženého objektu do výšky tak, aby byla nedostupná bez použití žebříku či štaflí.
Nejrozšířenějšími typy jsou tzv. inteligentní sirény s vlastním zálohováním. Siréna je propojena s ústřednou kabelem, který slouží k ovládání řídicího vstupu sirény, dobíjení zálohovacího akumulátoru a k přivedení sabotážní smyčky sirény.

Inteligentní siréna je aktivována v těchto případech:

- Poplach systému EZS,
- Přerušení kabelového spojení ústředna – siréna,
- Pokus o odstranění pláště sirény,
- Pokus o manipulaci sirény.

2.5.2 Optická signalizace (světelný maják)

Nejčastěji je součástí krytu venkovní sirény. Světelný maják je nejčastěji výbojka buzená vlastní elektronikou, nebo méně často výkonová 12V žárovka buzená přes elektronický přerušovač.

Zařízení by mělo umožňovat časově neomezenou aktivaci v případě vyhlášení poplachu. Důvodem je identifikace narušení i po doznění sirény v případě více střežených objektů umístěných blízko sebe.

2.5.3 Poplachová přenosová zařízení (komunikátory)

Komunikátory slouží pro ovládání, nastavení a monitorování EZS pomocí telefonní linky, mobilního telefonu nebo internetu. Do určité míry nesplňuje současná lokální akustická a optická signalizace dostatečné zabezpečení střeženého objektu. Jedná se především o situace, kdy je uživatel nepřítomen v době vyhlášení poplachu. Nedostatečným zabezpečením je myšlena především nulová informace o narušení objektu, nemožnost vzdáleného ovládání systému a jakéhokoli zásahu, rychlé upozornění pachatele a jeho obtížné dopadení a rušení okolního prostředí. Pro eliminaci těchto situací se využívá vzdálené signalizace vyhlášení poplachu. Tu je možné realizovat pomocí komunikátorů několika způsoby, které závisejí na přenosovém médiu.

a) Telefonní komunikátor

Jedná se o zařízení, které vzdáleně komunikuje s jinými ústřednami prostřednictvím jednotné telefonní sítě JTS. Komunikátor je většinou integrován na základní desce ústředny, nebo je řešen jako zásuvná karta do slotu ústředny.

Základní funkce telefonního komunikátoru:

- Reportování událostí zavoláním na telefonní přístroj a předání akustického signálu,
- Předávání dat na pult centrální ochrany PCO,
- Dálkové ovládání a programování sytému EZS
  - Zavoláním,
  - Pomocí SMS příkazů,
  - Tónovou volbou DTMF pomocí klávesnice,
  - Pomocí vzdáleného PC s tel. modemem pro vytáčené připojení.

b) GSM komunikátor

Jedná se o zařízení, které umožňuje stejné funkce jako telefonní komunikátor s tím rozdílem, že se vzdáleným zařízením komunikuje prostřednictvím sítě GSM. Opět je buď integrován přímo na základní desce ústředny, nebo v případě zásuvné karty zasunut do slotu základní desky. Používá se především s objektem bez telefonní linky JTS a je aplikován v podobě GSM brány.
Největší nevýhodou komunikace prostřednictvím GSM je, že mobilní operátoři nerozlišují priority SMS zpráv a poplachové hlášení tak může k majiteli dorazit s velkým časovým zpožděním. Další slabina může být zarušení přenosového pásma.

c) LAN komunikátor

Tento komunikátor slouží k propojení systému EZS se vzdáleným zařízením (PC, server, SMS brána) prostřednictvím sítě LAN. Za použití routeru (směrovače) je využito připojení prostřednictvím internetu.

Tento přenos nelze považovat za zcela bezpečný, je ovlivněn především zabezpečením samotné sítě poskytovatelem ISP.

d) Komunikace s pultem centrální ochrany PCO

Pult centrální ochrany PCO je zpravidla osobní počítač, ke kterému je připojena ústředna EZS, která mu zasílá poplachové informace. Tato zařízení umožňují přenos i vyhodnocení signalizace narušení ze zabezpečených objektů, zasílání informací o stavu EZS a jednotlivých čidlech, poruchách systému a rušení komunikace a informace o stavu baterie do místa centrálního vyhodnocení. V takovém případě je PCO vybaven softwarem, který tyto zprávy archivuje a umožní jejich zobrazení.

Komunikace probíhá pomocí určitého kódu, který obsahuje informace o objektu a typ předávané zprávy. Vyspělé systémy umožňují oboustrannou komunikaci, což umožňuje monitorování přenosové trasy.

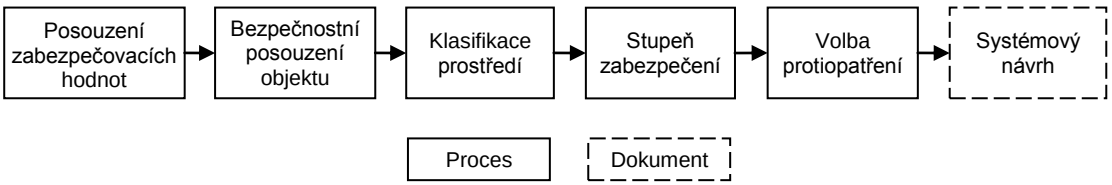
Spojení ústředny EZS s PCO lze uskutečnit několika způsoby (RS 232, SMS zpráva v GSM, modem po telefonní lince, internet).

3. NÁVRH EZS

Návrh systému EZS [1], [3], [5] je proces, při němž se stanovuje rozsah systému, stupeň zabezpečení, komponenty odpovídajícího stupně zabezpečení, volby protiopatření, třídy prostředí. Při tomto procesu dochází k výběru vhodné ústředny a způsobu provedení kabeláže, ke stanovení počtu a typu detektorů, typu ovládacích a indikačních zařízení a dalších doplňkových zařízení. Návrh systému EZS většinou také slouží pro přibližný odhad ceny navrhovaného systému.

3.1 Obecný návrh EZS

Na *Obrázku 3.1* je znázorněn sled událostí při návrhu EZS vycházející z [3].



Obrázek 3.1: Návrh systému EZS

Pro jednotlivé komponenty při návrhu systému EZS musí platit několik pravidel:

- Komponenty EZS musí být klasifikovány v souladu s jejich odolností vůči vlivům prostředí a děleny podle jejich provedení do stupňů zabezpečení,
- Komponenty EZS musí být v rámci EZS navzájem kompatibilní a musí být voleny v souladu se stupněm zabezpečení a příslušnou třídou prostředí,
- Komponenty jiných aplikací mohou být kombinovány nebo integrovány s EZS za předpokladu, že nedojde k negativnímu ovlivňování vlastností komponent EZS.

3.1.1 Posouzení zabezpečovacích hodnot

Při stanovení bezpečnostního stupně EZS objektu je nutné brát v úvahu tyto faktory:

- Druh majetku, snadnost zpeněžení, atraktivnost pro pachatele,
- Hodnota majetku, maximální hodnota ztráty, výdaje související se ztrátou, osobní ztráty,
- Objem nebo velikost majetku, snadnost krádeže a transportu,
- Historie krádeží, počet předešlých krádeží ve střežených objektech, způsob vloupání při předchozích krádežích,
- Nebezpečí pro okolní prostředí, zneužití střeženého majetku,
- Poškození vandalizmem na střeženém majetku, riziko žhářství.

3.1.2 Bezpečnostní posouzení objektu

a) Prověrka lokality budovy

Při systémovém posuzování hlavních rizik projektu EZS bude při jeho zpracování hlavním určujícím faktorem struktura střežených objektů.

Je nutné posoudit následující faktory:

- Konstrukce stěn, střech, podlah, sklepení,
- Otevírané části dveří, oken, střešních světlíků, ventilačních kanálů, ostatních otevíraných částí pláště budovy,
- Provoz (veřejná budova, přítomnost ostrahy),
- Lokalita (míra kriminality, okolní budovy usnadňující vniknutí, rychlost reakce na signalizaci, vzdálenost a informace o sousedních objektech),
- Stávající zabezpečení (kvalita a rozsah),
- Historie krádeží (počet předchozích krádeží, způsoby vloupání),
- Místní legislativy, předpisy (bezpečnostní požadavky, požární předpisy, konstrukce budovy),
- Poloha střeženého objektu (městská zástavba, venkov).

b) Faktory mající původ uvnitř střežených objektů

Uvnitř střežených objektů existuje řada faktorů, které mohou ovlivnit správnou funkci EZS. Při volbě typu zařízení, zvláště čidel a jejich umístění, je nutno tyto faktory posoudit.

Faktory, které mají původ uvnitř střežených objektů, lze považovat za ovlivnitelné uživatelem objektu. Pokud by dané podmínky mohly negativně ovlivnit provoz nějakého komponentu systému nebo celý systém, je nutno tyto podmínky změnit.

Mezi takové podmínky patří:

- Vodovodní potrubí (vliv pohybu vody v plastových potrubích na MW čidla),
- Tepelné, ventilační a klimatizační systémy (vliv turbulence na US čidla),
- Závěsné tabule a ostatní předměty (vliv pohyblivých částí na čidla),
- Výtahy (vliv vibrací způsobené výtahy a strojními zařízeními na čidla),
- Světla (vliv zářivek na MW čidla, vliv halogenových světel na PIR čidla),
- Elektromagnetické rušení (všechna elektrická zařízení jsou zdrojem elektromagnetického rušení, které může ovlivnit provoz zařízení EZS),
- Vnější zvuky (vlivy zařízení generující zvuky ve stejném frekvenčním rozsahu na US čidla – telefonní zvonky, letadla, kompresory),
- Domácí zvířata a škůdci (vliv na čidla pohybu i otřesová čidla),
- Průvan (vliv proudění vzduchu na PIR a US čidla – vznikají v důsledku špatně utěsněných otvorů),
- Uspořádání skladových předmětů (možnost zastínění průzoru čidel, možnost přemisťování skladovaných předmětů, zařízení interiéru v průzoru čidla),
- Struktura střežených objektů (při volbě umístění čidel nutnost posoudit strukturu střežených objektů a stav a usazení dveří a oken),

- Speciální pozornost (nutné odborné posouzení – hořlaviny, výbušniny, skelné podklady).

c) Faktory mající původ vně střežených objektů

Také vně střežených objektů se vyskytuje řada faktorů, které mohou ovlivnit provoz EZS. Rovněž tyto faktory je nutné posoudit při volbě typů zařízení a při rozmísťování těchto zařízení.

Za ovlivňující faktory mimo střežené objekty se považují takové, které uživatel nemůže ovlivnit. Pokud by dané podmínky mohly negativně ovlivnit provoz nějakého komponentu systému nebo celý systém, je nutno tyto podmínky změnit. *Mezi takové podmínky patří:*

- Dlouhodobé faktory (silnice, železnice, podzemní dopravní systémy, letecká doprava, parkoviště podzemní i nadzemní, zemětřesení a chvění půdy),
- Krátkodobé faktory (vliv konstrukce sousedících budov),
- Vlivy počasí (místa s výskytem silných větrů a dešťů, časté blesky),
- Vysokofrekvenční rušení (vliv blízkosti stožárů vysílačů, civilních antén, vojenských radarů, antén amatérských vysílačů na bezdrátové EZS),
- Sousední objekty (vliv činností, procesů a zařízení provozovaným nebo přepravovaným v těchto objektech na střežený objekt – vibrace, zařízení generující vysoké hladiny elektromagnetického rušení),
- Vlivy klimatických podmínek (nutné použít pouze zařízení vhodná pro dané klimatické podmínky – teplotní rozsah, relativní vlhkost nebo vlhko),
- Ostatní podmínky (aktivity v okolí).

3.1.3 Klasifikace prostředí pro zařízení

Jak již bylo zmíněno, je při výběru nutno zvážit prostředí, ve kterém budou jednotlivé komponenty systému EZS umístěny a ve kterém budou schopny správného a spolehlivého provozu. Toto rozdělení je znázorněno v *Tabulce 3.1*.

Tabulka 3.1: Třídy prostředí [1]

Třída	Název prostředí	Popis prostředí	Rozsah teplot
I	Vnitřní	Vytápěná obytná nebo obchodní místa	+5 až +40 °C
II	Vnitřní všeobecné	Přerušovaně vytápěná nebo nevytápěná místa (chodby, schodiště, sklady)	-10 až +40 °C
III	Venkovní chráněné	Prostředí vně budov, kde komponenty nejsou trvale vystaveny vlivům počasí	-25 až +50 °C
IV	Venkovní všeobecné	Prostředí vně budov, kde komponenty jsou trvale vystaveny vlivům počasí	-25 až +60 °C

3.1.4 Stupeň zabezpečení

Ke stanovení stupně zabezpečení je zapotřebí posouzení zabezpečovacích hodnot a bezpečnostního posouzení objektu. Toto posouzení se provádí vždy za účasti zákazníka, případně za účasti dalších zainteresovaných subjektů (policie, bezpečnostní agentura, pojišťovna). Orgánem, který toto posouzení provádí, bývá zpravidla zástupce organizace, která zajišťuje návrh systému EZS. Rozdělení stupňů zabezpečení je znázorněno v *Tabulce 3.2*.

Tabulka 3.2: Klasifikace stupně zabezpečení [1]

Stupeň	Míra rizika	Typ prostorů	Typ útočníka
1	Nízké	Obytné objekty s méně cennými aktivy	Útočník s malou znalostí EZS (omezený sortiment snadno dostupných nástrojů)
2	Nízké až střední	Kancelářské prostory, obytné objekty, komerční prostory	Útočník má omezené znalosti EZS (běžné nástroje a přenosné přístroje, např. multimetr)
3	Střední až vysoké	Banky	Útočník je obeznámen s EZS (rozsáhlý sortiment nástrojů a přenosných elektronických zařízení)
4	Vysoké	Tajné archivy, muniční sklady	Útočník má podrobný plán vniknutí (kompletní sortiment zařízení a přístrojů, včetně prostředků pro náhradu prvků EZS)

Ve všech stupních zabezpečení termín *útočník* zahrnuje i ostatní typy ohrožení (například loupežné přepadení nebo vyhrožování fyzickým násilím), což může ovlivnit návrh EZS.

3.1.5 Volba protiopatření

Pro každý stupeň zabezpečení je charakteristická konkrétní volba protiopatření. Pomůcka pro správný výběr protiopatření je znázorněna v *Tabulce 3.3*.

Tabulka 3.3: Pomůcka při stanovení volby protiopatření [6]

Možné narušení	Stupeň 1.	Stupeň 2.	Stupeň 3.	Stupeň 4.
Obvodové dveře	O	O	OP	OP
Okna		O	OP	OP
Ostatní otvory		O	OP	OP
Stěny				P
Stropy, střechy				P
Podlahy				P
Místnosti	T	T	T	T
Předměty (vysoké riziko)			S	S
O – otevření, P – průnik, T – nástraha, S – předmět vyžadující speciální posouzení				

Detekce *otevření* je nutné u okna nebo jiného otevíratelného prostoru, jehož rozměry jsou větší než 900cm^2 a jenže je umístěn ve vzdálenosti menší než 5,5m ve všech směrech od míst, z nichž by bylo možné vniknout do střeženého prostoru (balkon, lodžie, střecha, otevřený terén). Je realizováno většinou magnetickým či mechanickým kontaktem.
Detekce *průnikem* je nutná u otvorů větších než 900cm^2. Je realizováno většinou detektorem tříštění skla GBS nebo otřesovým čidlem.
U *nástrahy* je nutná detekce průchodu útočníka. Je realizováno většinou detektorem pohybu.
Potřeba *speciální* detekce je dána specifiky chráněných aktiv, kterými mohou být například umělecká díla.

3.1.6 Systémový návrh EZS

Je to dokument, který je výsledkem návrhu systému EZS. Zpracovává se jako podklad pro zadavatele nebo kupujícího. Tento návrh obsahuje všechny informace, podle kterých se zadavatel nebo kupující může přesvědčit o vhodnosti vybraného typu EZS pro danou aplikaci, účel a lokalitu.
V tomto dokumentu musí být uvedeny následující informace:

- Údaje o zákazníkovi (údaje nutné pro identifikaci zákazníka),
- Údaje o střežených objektech (název a adresa, popis – typ konstrukce, účel objektu – např. rodinný dům),
- Stupeň zabezpečení navrženého EZS,
- Třída prostředí každého komponentu EZS,
- Přehled komponentů (přehled typů, rozmístění, očekávané pokrytí),
- Konfigurace systému (programování smyček),
- Ohlašování (typ a umístění signalizačních zařízení, zařízení dálkového přenosu poplachu a název PCO),
- Legislativa (údaje o shodě komponentů systému s požadavky místní nebo národní legislativy),
- Normy (údaje o shodě prvků systému s požadavky národní nebo evr. normy),
- Další předpisy (podrobnosti o shodě komponentů systému s dalšími předpisy – směrnice, kódy publikované pojišťovnami nebo příslušnými inspektoráty),
- Certifikace (údaje o uplatnění nároku na certifikaci prvků i EZS systémů),
- Odezva (plánované odezvy na signalizaci poplachů nebo poruch – PČR, majitel, bezpečnostní agentura),
- Údržba a Opravy (údaje o plánované údržbě EZS a firmě poskytující servis).

3.2 Metodika návrhu EZS pro stupně zabezpečení 1 a 2

V předchozí kapitole byl popsán návrh systému EZS z obecného hlediska. Pro splnění zadání této práce je podstatné vytvořit metodiku návrhu pro stupeň

zabezpečení 1 a 2. Jedná se především o obytné objekty a méně cennými aktivy pro stupeň 1 a kancelářské prostory, obytné objekty a komerční prostory pro stupeň 2.

3.2.1 Posouzení zabezpečovacích hodnot / Stupeň zabezpečení

Při zjednodušení návrhu EZS pouze na stupeň zabezpečení 1 a 2 lze pomocí hodnoty aktiv rozhodnout, do jakého stupně zabezpečení daný objekt spadá. Krok *Posouzení zabezpečovacích hodnot* lze tedy sloučit s krokem *Stupeň zabezpečení*.
V návrhu bude určujícím faktorem hodnota majetku (aktiv), který má být zabezpečen a následné výdaje související s jeho ztrátou. Není jisté, že toto rozdělení bude vždy přesné a správné, pro současnou situaci je toto rozdělení dostačující. Záleží rovněž na přání zákazníka. Toto rozdělení je uvedeno v následující *Tabulce 3.4*.

Tabulka 3.4: Zjištění stupně zabezpečení objektu

Faktor	Hodnota	Stupeň 1	Stupeň 2
Hodnota majetku (aktiv), následné výdaje související se ztrátou	do 200.000 Kč	X	
	nad 200.000 Kč		X
X – platný výběr			

3.2.2 Bezpečnostní posouzení objektu / Volba protiopatření

Krok *Bezpečnostní posouzení objektu* nám v podstatě určuje faktory negativně ovlivňující komponenty systému EZS, které pomohou správně rozhodnout, jaký detektor, ústřednu a ostatní prvky EZS musí být vybrány, aby spolehlivost navrženého systému EZS byla co nejvyšší. Pro jednoduchost lze tento krok sloučit s krokem *Volba protiopatření*, který určuje počet detektorů.
Podstatou tohoto kroku je vybrat vhodný počet detektorů pohybů tak, aby pokryl celý střežený prostor a počet magnetických kontaktů tak, aby byly v závislosti na stupni zabezpečení zabezpečeny všechny vstupní otvory do objektu. Dále je nutné identifikovat faktory negativně ovlivňující činnost celého systému EZS a jeho prvků a na jejich základě vybrat vhodný detektor a ústřednu. Vychází se z informací uvedených v kapitolách *3.1.2 Bezpečnostní posouzení objektu* a *3.1.5 Volba protiopatření.*

a) Volba ústředny

Nejdříve je nutné vybrat vhodný typ ústředny, podle kterého budeme vybírat vhodné komponenty. Pro výběr vhodného typu ústředny je nutné, aby nebyla komunikace s komponenty EZS systému nijak rušena. Způsob výběru vhodného typu propojení ústředny s detektory je uvedeno v *Tabulce 3.5*.

Tabulka 3.5: Výběr vhodného propojení ústředny s detektory [3]

Faktor	kabelové	bezdrátové
Elektromagnetické rušení (výbojky, generátory, souběhy kabelů)	X	
Vysokofrekvenční rušení, velké kovové předměty (stěny, přepážky)		X
X – není možné použít tento typ propojení		

b) Volba detektorů

Z *Tabulky 3.3* je vidět, že pro spolehlivé zabezpečení objektu stupně 1 je nutné detekovat otevření obvodových dveří, což je realizováno magnetickým kontakty a detekovat pohyb ve všech místnostech objektu kromě sociálního zařízení (WC, koupelna), což je realizováno detektory pohybu.

Pro spolehlivé zabezpečení objektu stupně zabezpečení 2 je nutné detekovat otevření nejen obvodových dveří, ale také všech oken a ostatních otevíratelných otvorů (vrata), což je realizováno magnetickým kontakty. Detekce pohybu je opět realizována detektory pohybu ve všech místnostech vyjma sociální zařízení.

Pro návrh zabezpečení je nejdůležitější výběr vhodného typu pohybového detektoru. Jak již bylo několikrát zmíněno, pro instalaci a používání každého typu detektoru platí určitá pravidla a opatření, díky nimž je riziko vyvolání falešných poplachů minimalizováno či eliminováno. Zjednodušený a dostačující přehled použití jednotlivých detektorů je znázorněn v *Tabulce 3.6*.

Tabulka 3.6: Výběr správného typu pohybových čidel

Faktor	PIR	MW	US
Vodovodní plastové potrubí		X	
Zářivkovité osvětlení samostatně spínané v době střežení		X	
Halogenová světla samostatně spínané v době střežení	X		
Spínané rušivé IR zářivky	X		
Tepelné, ventilační, klimatizační systémy (turbulence vzduchu)	X		X
Prudké změny teploty (podlahové vytápění, komíny)	X		X
Volně zavěšené předměty (lampy)			X
Zvuky se širokým kmit. spektrem (telefonní zvonky, kompresory)			X
X – není možné použít tento detektor			

Dalším krokem je zjištění počtu potřebných pohybových detektorů a magnetických kontaktů a na nich závislý typ použité ústředny.

Počet pohybových detektorů se odvíjí od počtu místností střeženého objektu, ve kterých je nutné detekovat pohyb. Jedním detektorem lze pokrýt prostor o rozloze přibližně 150 m^2. V případě větších místností je potřeba použít detektorů více. Počet

magnetických kontaktů se odvíjí podle počtu samostatně otevíratelných křídel dveří, oken a ostatních obvodových prostupů.

Tabulka 3.7: Určení počtu detektorů

Stupeň	Počet detektorů pohybu	Počet magnetických kontaktů
1	Počet místností + chodby + garáže	Počet otevíratelných křídel dveří
2	Počet místností + chodby + garáže	Počet otevíratelných křídel dveří + oken

c) Volba ostatních a doplňkových komponent

Výběr typu klávesnice a signalizačního zařízení závisí na propojení s ústřednou a na možnostech zákazníka, stejně jako vhodný počet. Klávesnice by měla být umístěna u každého vstupu do objektu (hlavní vchod, garáž), signalizační zařízení se nejčastěji umísťují na průčelí střeženého objektu do výšky tak, aby byla nedostupná bez použití žebříku či štaflí.
S ústřednou je nutné také vhodně zvolit záložní akumulátor a případně komunikátor, který slouží pro ovládání, nastavení a monitorování EZS pomocí telefonní linky, mobilního telefonu nebo internetu, nebo přeposílání informací na PCO.

3.2.3 Klasifikace prostředí pro zařízení

Tento krok lze při návrhu EZS pouze pro první dva stupně zabezpečení teoreticky vypustit, protože všechny prvky, které je při návrhu nutné podrobit pečlivému výběru (ústředna, detektory, magnetické kontakty), musí být instalovány uvnitř střeženého objektu, kterému odpovídají třídy prostředí I. (vnitřní) a II. (vnitřní všeobecné). Většina současných komponent pro zřizování EZS pracuje v rozsahu teplot -10 až +40 °C, což splňuje provoz pro třídu prostředí II.
Venkovní siréna ovšem musí splňovat vyšší třídu prostředí (III. nebo IV.) pro venkovní provoz. Výběr této komponenty bude, jak již bylo zmíněno, závislé na zákazníkovi a není tedy nutné se touto komponentou nyní zabývat.

3.2.4 Systémový návrh EZS

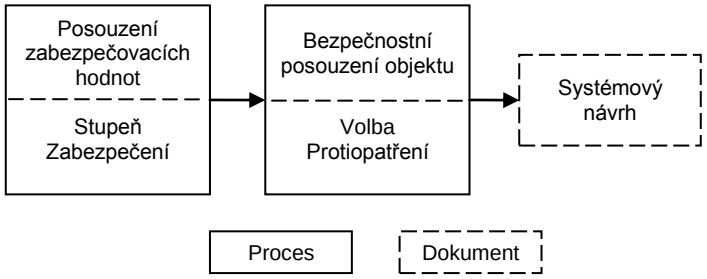
Systémový návrh by tedy měl obsahovat stejné údaje, jako obecný návrh. *Nejdůležitější informace pro tento návrh přitom jsou:*

- Údaje o zákazníkovi (údaje nutné pro identifikaci zákazníka),
- Údaje o střežených objektech (název a adresa, popis – typ konstrukce, účel objektu – např. rodinný dům),
- Stupeň zabezpečení navrženého EZS,
- Třída prostředí každého komponentu EZS,
- Přehled komponentů (typ, rozmístění, očekávané pokrytí, specifikace).

Další důležité údaje se vyplňují až při samotné realizaci návrhu.

3.2.5 Vývojový diagram návrhu EZS pro stupeň 1 a 2

Z informací a údajů uvedených v předchozích kapitolách lze tedy metodiku návrhu EZS pro objekty stupně zabezpečení 1 a 2 zjednodušit sloučením některých kroků, nebo jejich vypuštěním, jak je znázorněno na *Obrázku 3.2*.



Obrázek 3.2: Návrh systému EZS pro stupeň zabezpečení 1 a 2

4. PROGRAMOVÉ ŘEŠENÍ NÁVRHU EZS

Vytvořené programové řešení je založeno na webových technologiích. Výsledkem praktické části práce je webová stránka, na které se návštěvník dozví nejen o nezbytných základech EZS, jeho architektuře a komponentech a o samotném postupu při návrhu EZS, ale bude mít především možnost si sám vytvořit textový a grafický návrh EZS pro stupeň zabezpečení 1 a 2, který může použít jako předlohu pro zabezpečení svého objektu.

4.1 Použité technologie a nástroje

Webová stránka je vytvořena v redakčním systému Drupal s implementovaným modulem FCKeditor (WYSIWYG editor). Textový návrh vznikl za použití jazyka PHP a MySQL. Grafický návrh vznikl za použití programů Adobe Flash a Adobe Flex Builder.
Technologie a programy použité pro vytvoření a fungování programového řešení návrhu EZS byly vybrány z důvodu výkonnosti, rychlosti a uživatelské jednoduchosti. Všechny tyto programy jsou bezplatné nebo je lze zdarma využívat po omezenou dobu.

4.1.1 Drupal

Drupal [7] je open source redakční systém, tedy volně dostupný software, který umožňuje jedincům nebo skupinám uživatelů snadno publikovat, spravovat a uspořádat širokou škálu obsahu na webových stránkách. Staví na několika základech, které jsou důležité pro jeho fungování a vývoj:

- *Modularita* – diskuzní stránky, firemní weby, intranetové aplikace, sociální sítě, blog, osobní stránky, e-shop, korporátní web – to vše Drupal umožňuje díky svému modulárnímu systému: Malé, ale stabilní a rychlé jádro s dobrým rozhraním a moduly, na kterých staví. Každý může vytvořit vlastní modul, seznam modulů je udržován na domovské stránce Drupalu.
- *Kvalita* – Do jádra Drupalu se nedostávají neověřené patche, jádro má rovněž velmi dobře navrženou strukturu. To z něj dělá bezpečný a stabilní systém.
- *Open Source* – GNU/GPL licence, PHP programovací jazyk, podpora pro MySQL a PostgreSQL, připravovaná podpora pro MS SQL a Oracle.

V základní instalaci Drupalu jsou obsaženy moduly pro tvorbu článků, statických stránek, diskusních fór, blogů, přidávání komentářů k obsahu a mnoho dalších. Všechny tyto moduly můžete zapnout po instalaci na stránce Administrace → Moduly. Další funkcionalitu je možné přidat pomocí stažených modulů, jejich seznam naleznete na stránkách Drupal.org.

4.1.2 PHP

PHP (rekurzivní zkratka PHP Hypertext Preprocessor, původně Personal Home Page) je skriptovací programovací jazyk, který je určený především pro programování dynamických Internetových stránek. Nejčastěji se začleňuje přímo do struktury jazyka HTML či XHTML, což je velice výhodné pro tvorbu webových aplikací. PHP lze ovšem použít také k tvorbě konzolových a desktopových aplikací.
PHP skripty jsou prováděny na straně serveru a k uživateli je přenášen až výsledek jejich činnosti. PHP je nezávislý na platformě, skripty proto fungují bez úprav na mnoha operačních systémech. Jazyk obsahuje rozsáhlé knihovny funkcí pro zpracování textu, grafiky, práci se soubory, přístup k databázovým serverům (MySQL, PostgreSQL, MSSQL) a podporu celé řady Internetových protokolů (HTTP, SMTP, SNMP, FTP, IMAP, POP3, atd.)
Jazyk PHP se stal velmi oblíbeným především díky jednoduchosti použití a tomu, že kombinuje vlastnosti více programovacích jazyků a nechává vývojáři částečnou svobodu v syntaxi. V kombinaci s databázovým serverem (především s MySQL) a webovým serverem Apache je často využíván k tvorbě webových aplikací.

4.1.3 MySQL

MySQL je multiplatformní databáze. Komunikace s ní probíhá pomocí jazyka SQL (Structured Query Language). Podobně jako u ostatních SQL databází se jedná o dialekt tohoto jazyka s některými rozšířeními.
Pro svou snadnou implementovatelnost (lze jej instalovat na operační systém Linux, Microsoft Windows, Mac OSX a další operační systémy), výkon a především díky tomu, že se jedná o volně šiřitelný software, má vysoký podíl na v současné době používaných databázích. Velmi oblíbená a často nasazovaná je kombinace MySQL, PHP a Apache jako základní software webového serveru.
MySQL bylo od počátku optimalizováno především na rychlost, a to i za cenu některých zjednodušení: má jen jednoduché způsoby zálohování.

4.1.4 Apache

Apache HTTP Server je softwarový webový server s otevřeným kódem pro operační systém Linux, Microsoft Windows a další platformy. Název vznikl z anglického slovního spojení *"A patchy server"* (záplatovaný server). Jako indiánský symbol je ve znaku ptačí pero. V současné době dodává prohlížečům na celém světě většinu Internetových stránek.

4.1.5 Adobe

a) Flash

Flash [8] je grafický vektorový program ve vlastnictví společnosti Adobe (dříve Macromedia). Používá se především pro tvorbu internetových interaktivních

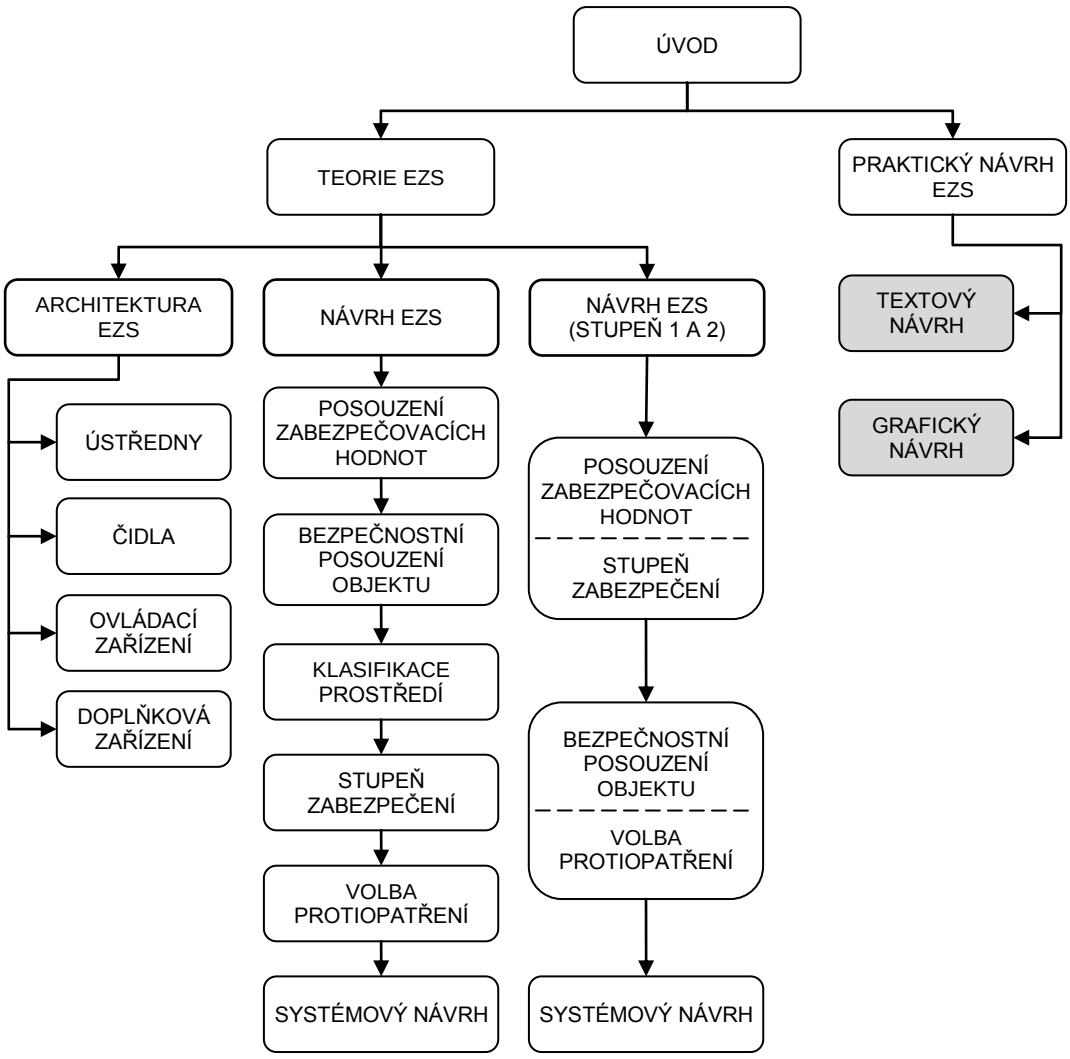
animací, prezentací a her. Rozšíření Flashe na internetu pomohla malá velikost výsledných souborů, protože se uchovávají ve vektorovém formátu, a proto vytlačily klasické flashové bannery, dříve používané ve formátu GIF.
Flash má také vlastní implementovaný programovací jazyk ActionScript, který slouží k rozvinutí všech možností interaktivní animace a vývoji robustních aplikací, v aktuálních verzích je ActionScript poměrně vyspělý objektově orientovaný programovací jazyk.

b) Flex

Flex [8] je bezplatný open source rámec pro budování vysoce interaktivních webových aplikací, který lze nasadit pro všechny hlavní prohlížeče a operační systémy. Poskytuje moderní, standardně založený jazyk a programovací model, který podporuje společné návrhové vzory. MXML, deklarativní XML jazyk, se používá pro popis vzhledu a chování, a ActionScript, výkonný programovací jazyk, je použit k vytvoření klienta logiky. Flex také zahrnuje bohaté knihovny s více než 100 komponentů k vytváření RIA (Rich Internet Application), stejně jako interaktivní aplikace Flex debugger. RIA vytvořené pomocí Flex lze spustit v prohlížeči pomocí Adobe Flash Player.

4.2 Webová stránka

Na *Obrázku 4.1* je hierarchicky znázorněna vytvořená webová stránka. Na úvodní stránce je kromě názvu projektu a jména autora popsán také důvod, proč projekt vznikl, jaký je jeho účel a co vše návštěvníkovi nabízí.
Zde má návštěvník možnost se rozhodnout, zda se chce nejdříve teoreticky seznámit se systémem EZS, nebo zda přejde rovnou k praktickému návrhu EZS stupně zabezpečení 1 a 2.
Vytvořená webová stránka je dostupná online na adrese http://ezs.labskalouka.cz.



Obrázek 4.1: Hierarchické znázornění webové stránky

4.2.1 Teorie EZS

V této části má návštěvník možnost seznámit se základy architektury a návrhem EZS. Tato část je určena především laikům, kteří zatím nemají o EZS žádné, nebo minimální informace a chtějí se před samotným návrhem dozvědět, jak elektronické zabezpečovací systémy vypadají, z jakých komponent se skládají a získat přehled o principech, vlastnostech a pokynech pro jejich používání a z jakých kroků se skládá návrh EZS.

a) Architektura EZS

Na této stránce jsou zobrazeny základní informace o architektuře a komponentách EZS. Tato stránka je určena především těm, kteří se chtějí podrobně seznámit s jednotlivými komponenty EZS. Je zde popsán princip jejich fungování, zásady pro instalaci a správnou funkci a funkce, které od komponent můžeme očekávat. Stránka je rozdělena na několik částí, kde každá z nich se věnuje jinému typu komponent. V každé části jsou kromě základních informací zobrazeny také obrázky daných komponent.

b) Návrh EZS

Na této stránce se návštěvník podrobně seznámí s návrhem EZS a s kroky, které je nutné podstoupit pro určení stupně zabezpečení a třídy prostředí, pomocí kterých se realizuje výběr vhodných komponent EZS, které zajistí spolehlivou funkčnost a ochranu střeženého objektu. Mezi tyto kroky patří posouzení zabezpečovacích hodnot a bezpečnostní posouzení objektů. Bude zde popsáno, jaké faktory a jakým způsobem objekt ovlivňují.

Informace použité na stránkách návrhu EZS vychází z kapitoly *3.1 Obecný návrh EZS*. Návštěvník tak bude proveden návrhem krok po kroku tak, jak by probíhal skutečný návrh a bude mít možnost zjistit, jaké stupně zabezpečení existují a k jakým typům objektů, míry rizika a pachatelů se vztahují. Dále se dozví, v jakých třídách prostředí můžou detektory pracovat, aby jejich funkce nebyly ovlivňovány, a podle jakých parametrů se jednotlivé komponenty vybírají. Výsledkem je systémový návrh, který obsahuje informace o zákazníkovi, objektu, komponentách EZS a další důležité informace.

c) Návrh EZS pro stupeň zabezpečení 1 a 2

Zde se návštěvník podrobně seznámí s navrženou metodikou pro návrh EZS pro stupeň zabezpečení 1 a 2. Informace použité na stránkách návrhu EZS vychází z kapitoly *3.2 Návrh EZS pro stupeň zabezpečení 1 a 2*.

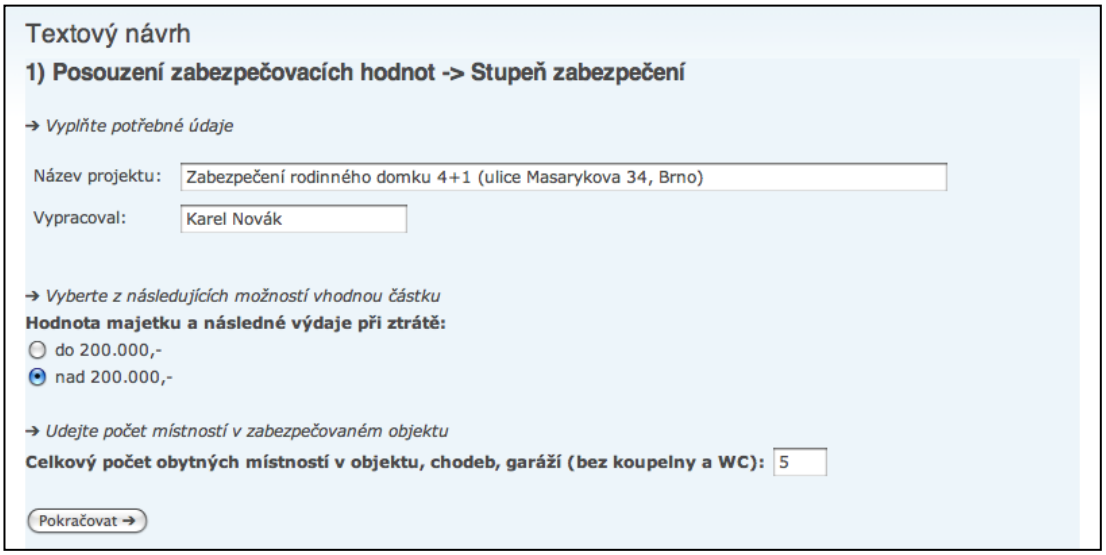
4.2.2 Praktický návrh EZS pro objekty stupně zabezpečení 1 a 2

Pokud návštěvník nepotřebuje teoretické informace o systému EZS a metodice jeho návrhu, může přejít přímo k samotnému praktickému návrhu EZS, který vychází

z kapitoly *3.2 Návrh EZS pro stupeň zabezpečení 1 a 2*. Stránka je rozdělena na dvě hlavní části, *textový návrh* a *grafický návrh*.
Pro kompletní a kvalitní návrh je potřeba nejdříve vytvořit textový návrh, ve kterém se vybere správný počet místností pro zabezpečení, negativní faktory ovlivňující činnost EZS a vhodné komponenty EZS a zjistí se jejich aktuální cena (systémový návrh). Tyto informace budou potom využity pro kvalitní grafický návrh.

a) Textový návrh

Textový návrh se skládá ze tří hlavních kroků, které jsou případně rozděleny.
V prvním kroku (*Posouzení zabezpečovacích hodnot / Stupeň zabezpečení*) uživatel vyplní vstupní informace, jako je *Název projektu* (např. Zabezpečení rodinného domku 4+1 - novostavba, ulice Masarykova 34, Brno) a *Vypracoval* (např. Karel Novák). Dále uživatel odhadne, jakou hodnotu má jeho majetek (má na výběr ze dvou hodnot, na základě kterých bude určen vhodný stupeň zabezpečení) a do jaké výše by sahaly výdaje při ztrátě. Posledním úkolem bude určení správného počtu místností, které je nutné zabezpečit. Mezi tyto místnosti spadají všechny místnosti (WC, koupelna), chodby a garáže. Tyto informace odešle tlačítkem *Pokračovat*.



Obrázek 4.2: Založení projektu EZS

Další krok (*Bezpečnostní posouzení objektu / Volba protiopatření*) je rozdělen do tří částí.

- ***Volba ústředny***

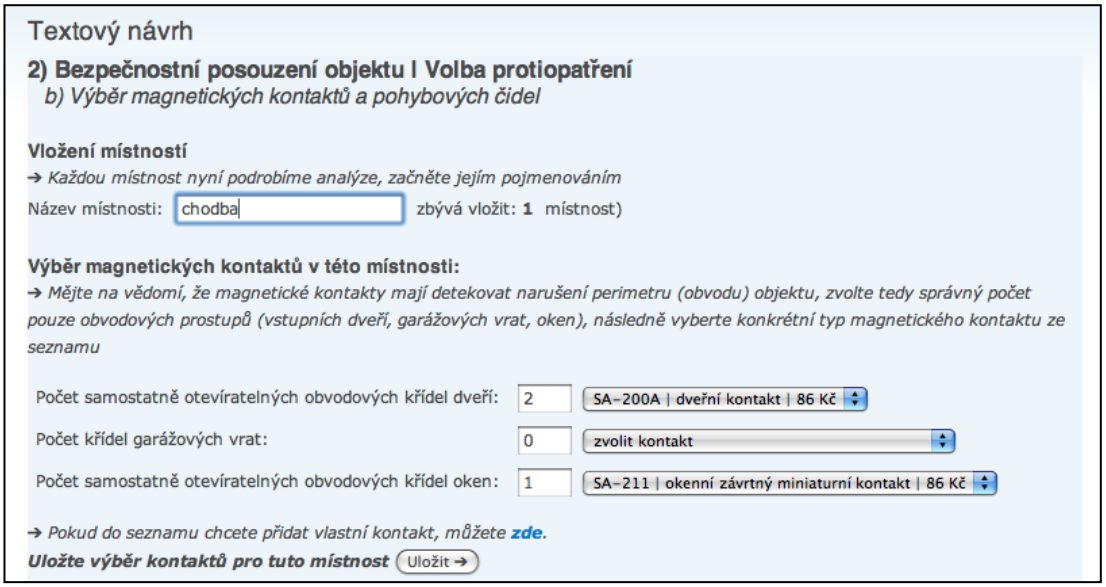
Volba ústředny probíhá na základě výběru faktoru negativně ovlivňujícího činnost ústředny podle *Tabulky 5*. Na základě tohoto výběru a jeho potvrzení budou uživateli zobrazeny možné typy propojení komponent EZS s ústřednou, které jsou: drátové, bezdrátové nebo hybridní (kombinace drátových i bezdrátových vstupů). Následně je uživateli zobrazen seznam všech vyhovujících ústředen v databázi, ze které si uživatel vybere podle získaných informací a podle svého uvážení. Pokud v seznamu není ústředna vyhovující požadavkům uživatele, má možnost do této databáze prvky přidávat. Výběr uloží tlačítkem *Pokračovat*.

Obrázek 4.3: Volba ústředny a typu propojení

- ***Volba detektorů***

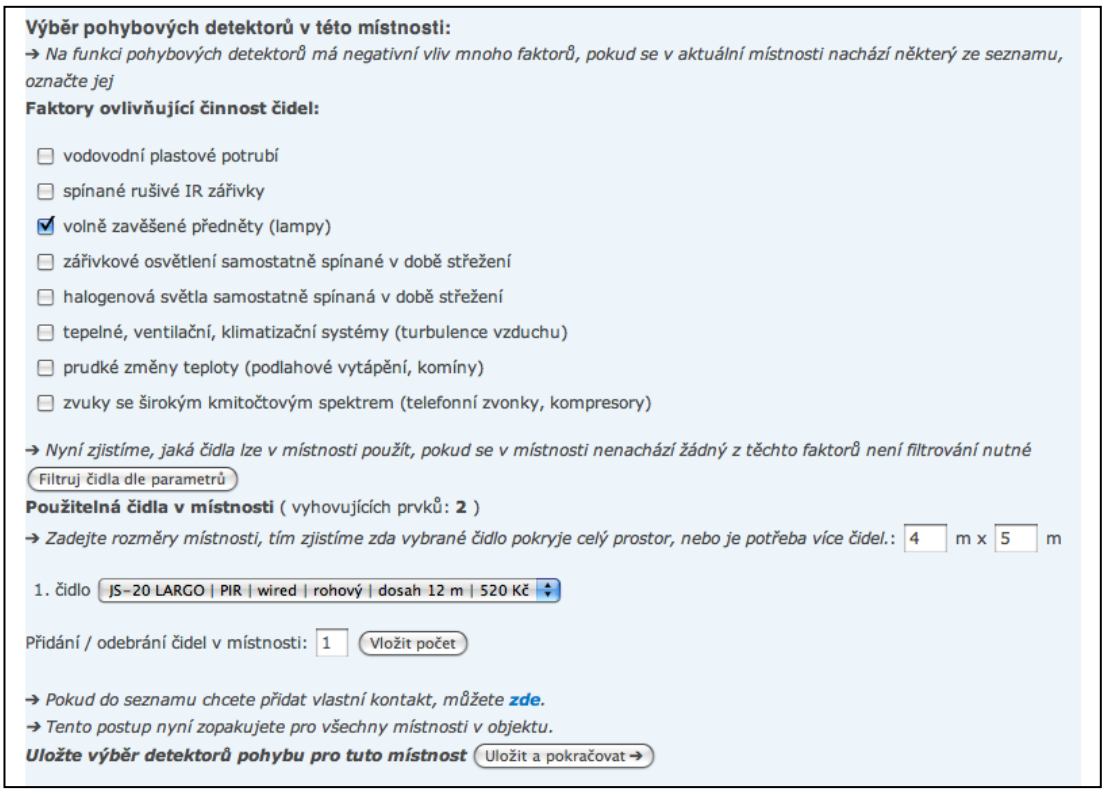
Počet místností k zabezpečení je již znám, teď je potřeba v každé místnosti určit vhodný počet magnetických kontaktů a detektorů pohybu a jejich vhodný typ. Vhodné propojení s ústřednou již také známe.

Nejprve se místnost označí názvem. Poté se zjistí vhodný počet magnetických kontaktů pro jednotlivé prostupy v *závislosti na stupni zabezpečení*, zapíše se do příslušných polí a vybere se konkrétní typ kontaktu. Pro každé samostatně otevíratelné křídlo je potřebný jeden magnetický kontakt. Opět je zde možnost do databáze přidat vlastní prvek. Výběr kontaktů se uloží tlačítkem *Uložit.*



Obrázek 4.4: Výběr magnetických kontaktů

Volba konkrétního typu pohybového čidla probíhá na základě výběru faktoru negativně ovlivňujícího činnost čidla podle *Tabulky 6*. Po označení přítomných faktorů vyfiltrujeme použitelný typ pohybového detektoru tlačítkem *Filtruj čidla dle parametrů*.



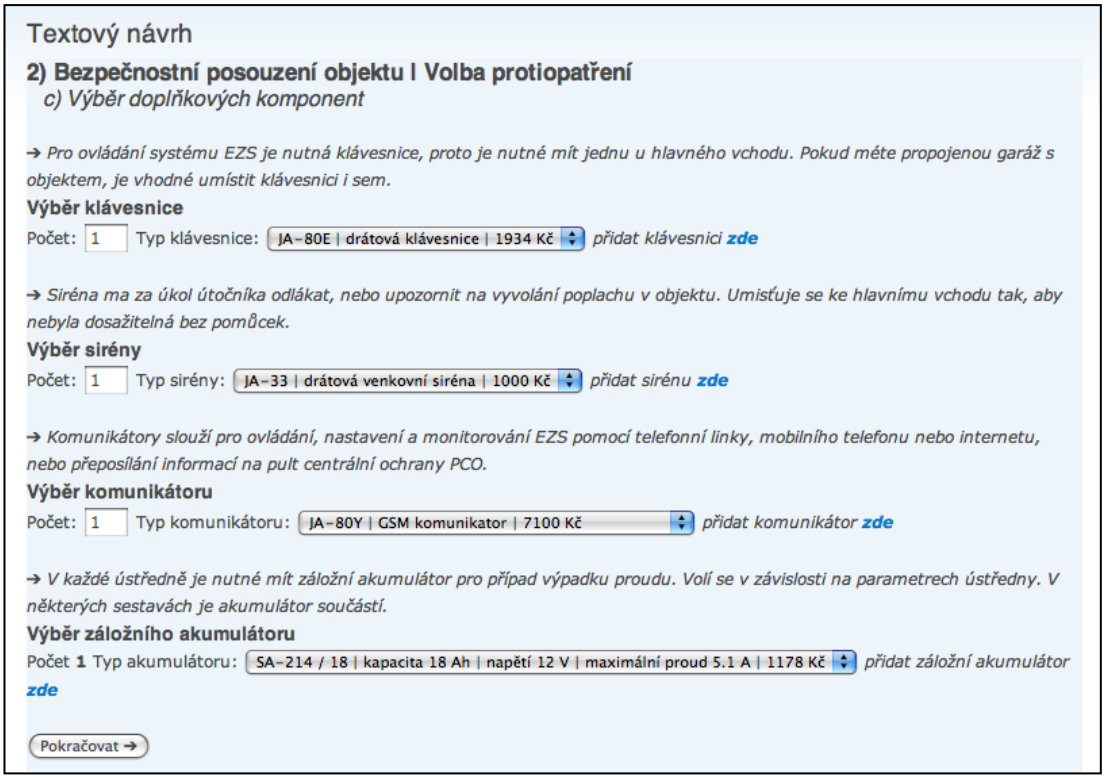
Obrázek 4.5: Volba pohybových detektorů

Po vyfiltrování uživatel zjistí, který typ pohybového čidla je možné použít. Mezi typy čidel patří: infračervené PIR, ultrazvukové US a mikrovlnné MW. V objektu je možné použít všechny typy současně, musí ale splňovat zásady správné instalace. V současné době jsou k dostání téměř výhradně infračervená pohybová čidla, která jsou pro zabezpečení objektů stupně 1 a 2 standardní, dostačující i doporučená.
Dále je nutné zjistit vhodný počet pro spolehlivé pokrytí celé místnosti. Každé čidlo má jiný dosah a rádius zorného pole. Tyto hodnoty se obvykle pohybují mezi 9 – 12 metry pro dosah a 90° – 120° pro rádius zorného pole pro PIR čidla použitelná do rohů místností, které jsou nejpoužívanější. Samozřejmě lze použít i jiná čidla, je však nutné je nejdříve přidat do databáze.
Po výběru konkrétního čidla ze seznamu nabízených čidel je tedy nutné zhodnotit, zda je jedno čidlo dostačující. To zjistíme z výpočtu úhlopříčky místnosti, tento výpočet bude možné provést přímo v návrhu. Do příslušných polí se zadají rozměry místnosti, vybere se konkrétní typ čidla ze seznamu, a pokud dané čidlo nepokryje tuto místnost, vyskočí tabulka s informací, že je nutné vybrat jiné čidlo s větším dosahem nebo více čidel. Počet čidel lze měnit pomocí tlačítka *Změnit počet* a napsáním tohoto počtu do příslušného pole. Po této volbě bude možné vybrat další pohybové čidlo. Je-li aktuální místnost kompletní, tzn. místnost má správně vybrané

množství a typy magnetických kontaktů a pohybových čidel, uloží se tlačítkem *Uložit a pokračovat*. Tyto kroky se nyní podstoupí pro každou zabezpečovanou místnost.

- ***Volba doplňkových komponent***

Po uložení všech místností následuje výběr doplňkových komponent systému EZS. Mezi tyto komponenty patří ovládací zařízení (klávesnice), signalizační zařízení (siréna, světelná siréna), komunikátory, záložní akumulátory a další prvky jako např. klíčenka.
Typ klávesnice je vybrán na základě propojení s ústřednou. Počet klávesnic záleží na požadavcích a finančních možnostech uživatele. Doporučuje se mít jednu klávesnici u každého hlavního vchodu a v garáži.
Siréna se nejčastěji umísťuje na průčelí střeženého objektu do výšky tak, aby byla nedostupná bez použití žebříku či štaflí. Typ sirény závisí na propojení s ústřednou. Konkrétní výběr signalizačního zařízení rovněž záleží na uživateli. Siréna není nutná, ovšem její instalace se doporučuje.
Komunikátory slouží pro ovládání, nastavení a monitorování EZS pomocí telefonní linky, mobilního telefonu nebo internetu, nebo přeposílání informací na PCO. Doporučuje se komunikátor použít v každém systému EZS.
V každé ústředně je nutné mít záložní akumulátor pro případ výpadku proudu. Volí se v závislosti na parametrech ústředny. V některých sestavách je akumulátor součástí.



Obrázek 4.6: Volba doplňkových komponent

Posledním krokem je *Systémový návrh*, kde budou zobrazeny shrnující informace o zabezpečovaném objektu.


Textový návrh

3) Systémový návrh

Název projektu: **Zabezpečení rodinného domku 4+1 (ulice Masarykova 34, Brno)**
Stupeň zabezpečení: **2**
Vypracoval: **Karel Novák**
Typ propojení ústředny s prvky: **Hybridní**
Typ ústředny : ústředna JA-83K (10 drátových vstupů), cena: **2618 Kč**

Místnosti:
chodba
Magnetické kontakty:
dveřní - počet: 2, typ: SA-200A, cena/ks: 86 kč, celkem: **172 Kč**
okenní - počet: 1, typ: SA-211, cena/ks: 86 kč, celkem: **86 Kč**
Pohybová čidla:
drátový PIR detektor - typ: JS-20 LARGO, cena/ks: **520 Kč**

Doplňkové komponenty
drátová klávesnice - typ: JA-80E, počet: 1, cena: **1934 Kč**
drátová venkovní siréna - typ: JA-33, počet: 1, cena: **1000 Kč**
GSM komunikator - typ: JA-80Y, počet: 1, cena: **7100 Kč**

Záložní akumulátor:
typ: SA-214 / 18, počet kusů: 1, cena: **1178 Kč**, kapacita: 18 Ah, napětí: 12 V, proud: 5.1 A

Cena
Cena za komponenty EZS: **14 608,00 Kč**
Cena za instalaci a zaškolení obsluhy ústředny: **4 000,00 Kč** (liší se od výrobce)

Obrázek 4.7: Systémový návrh EZS

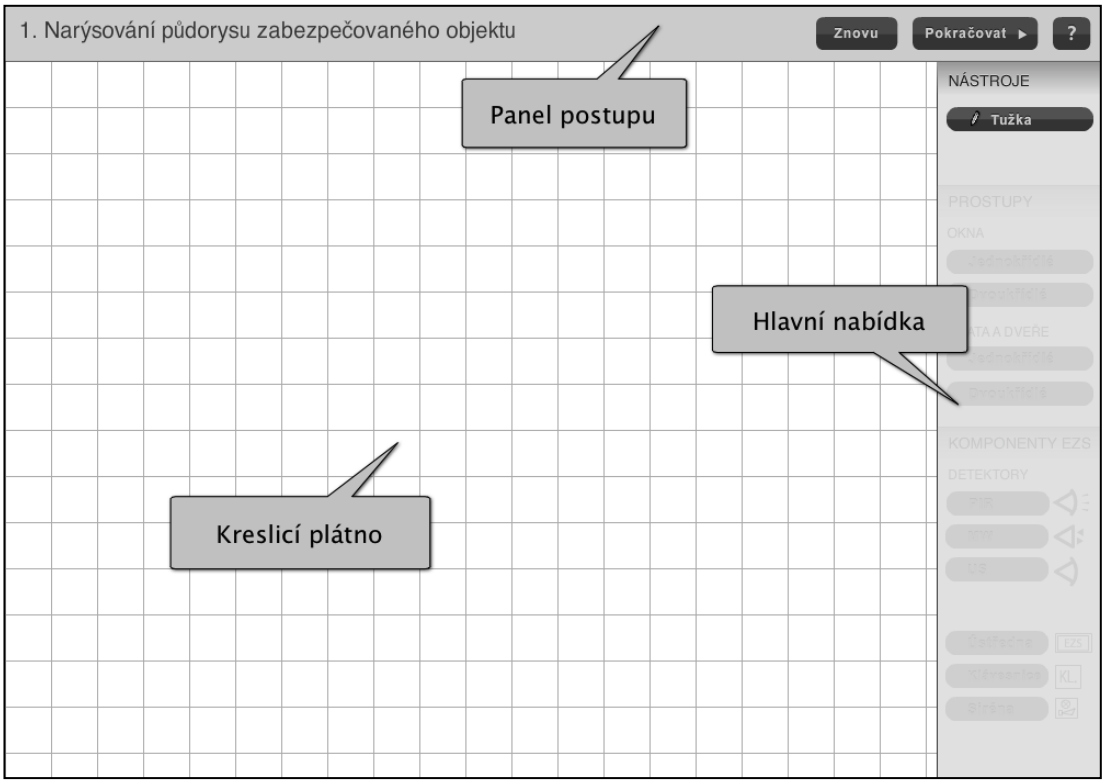
Tento návrh si nyní můžete vytisknout pomocí vašeho prohlížeče nebo uložit do formátu, který vám prohlížeč nabízí.

b) Grafický návrh

Grafický návrh byl vytvořen pomocí programu Adobe Flash a Adobe Flex Builder v programovacím jazyku ActionScript.
Před grafickým návrhem bude uživateli nabídnuta možnost ukázky vzorového návrhu EZS pro větší názornost.

Grafický návrh je založen na grafickém rozhraní, které uživateli umožní na grafické plátno zakreslit půdorys objektu, vyznačit v tomto půdoryse všechny místnosti a chodby, vyznačit všechny obvodové prostupy (okna, dveře, garážová vrata), které se mají zabezpečit v závislosti na stupni zabezpečení a do takto vytvořeného objektu správně vložit potřebné komponenty EZS tak, aby splňovaly zásady instalace a správné funkce. To vše za pomoci interaktivního průvodce, který se zobrazí vždy na začátku každého kroku, nebo po kliknutí na symbol otazníku **?**, který je umístěn v *panelu postupu* vpravo.

Grafické rozhraní se skládá ze tří hlavních částí:



Obrázek 4.8: Grafické rozhraní

- ***Kreslicí plátno***

Na kreslicí plátno s mřížkou je možné rýsovat, vkládat popisky místností a vybrané komponenty EZS.

- ***Panel postupu***

V panelu postupu je vypsán aktuální krok grafického návrhu, ve kterém se uživatel nachází a bude v něm stručný popis, co má uživatel v daném kroku udělat. Dále obsahuje tlačítko *Znovu*, které umožní aktuální krok vymazat a začít znovu, bez smazání předchozího kroku, tlačítko *Pokračovat*, které aktuální krok uloží a nabídne nápovědu pro následující krok a tlačítko pro nápovědu pro aktuální krok.

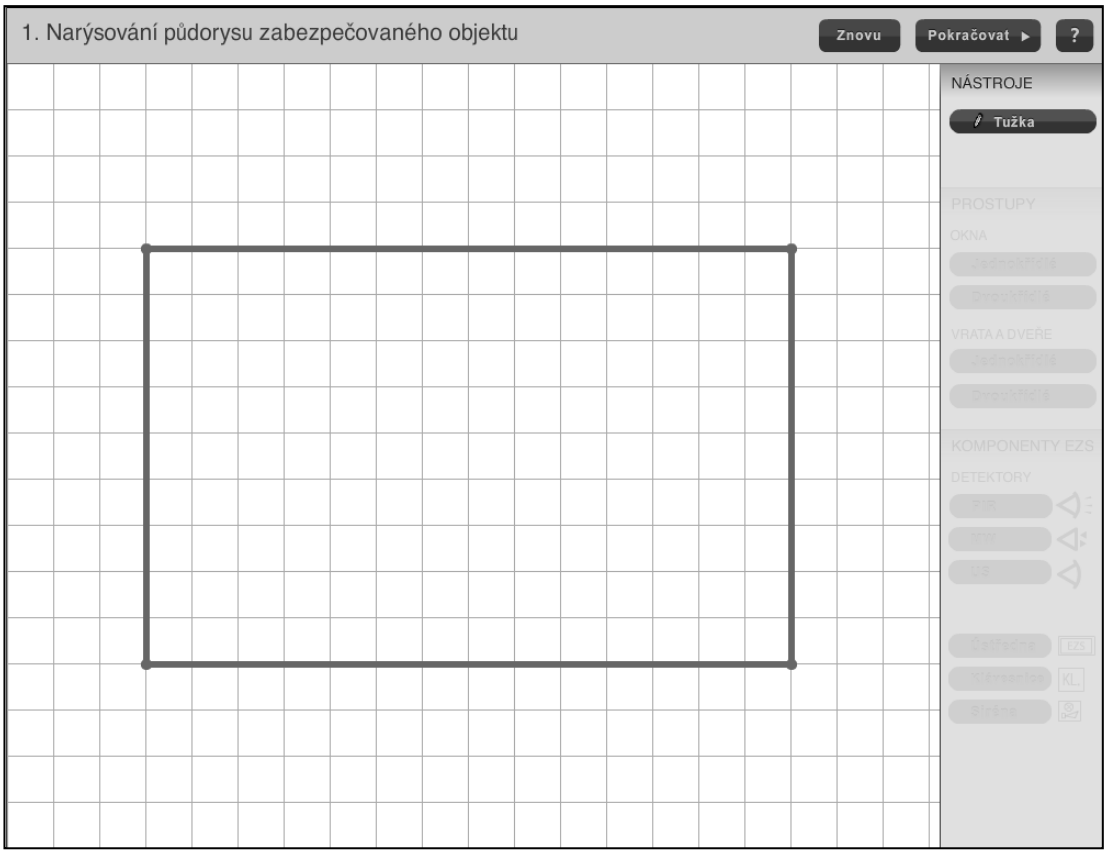
- ***Hlavní nabídka (menu)***

Menu je rozděleno na tři podmenu: nástroje, prostupy a komponenty EZS. V podmenu *Nástroje* je uživateli zobrazeno, že právě používá nástroj *Tužka*.
V podmenu *Prostupy* uživatel vybírá prostupy, které můžou mít jedno, nebo více samostatně otevíratelných křídel a které bude vkládat pouze na obvodové stěny půdorysu.
V podmenu *Komponenty EZS* uživatel vybírá jednotlivé komponenty EZS, které bude vkládat do objektu pomocí interaktivní nápovědy tak, aby splnily všechny zásady instalace.

Grafický návrh návrh se skládá ze čtyř kroků:

1) Narýsování půdorysu zabezpečovaného objektu

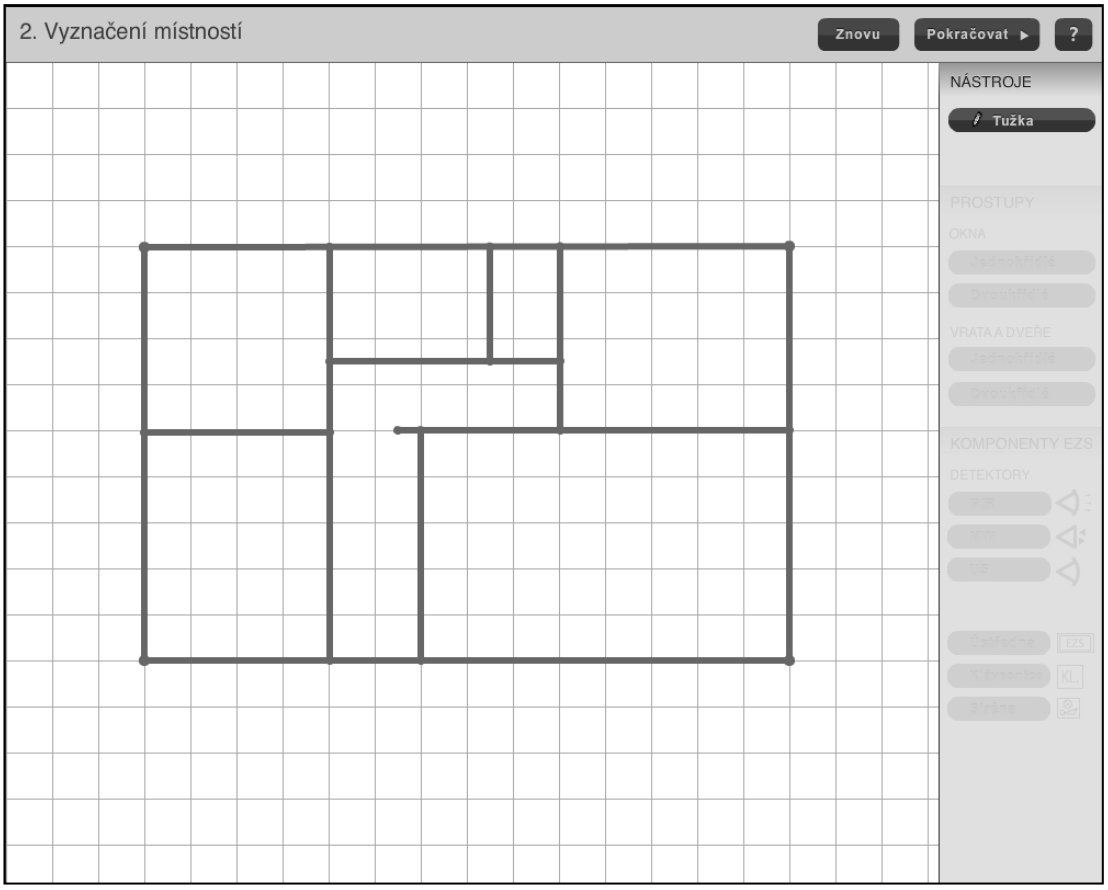
Půdorys objektu se kreslí spojitou čárou jako polygon. Uživatel začne rýsovat v počátečním bodě a v tomto bodě náčrt půdorysu také ukončí. Rovné čáry ve směru pohybu kurzoru dosáhne přidržením klávesy *Shift*. Při pohybu kurzoru po plátně se vedle kurzoru zobrazí také vzdálenost od posledního bodu v metrech v poměru k měřítku. Pokud není uživatel spokojen, může půdorys vymazat tlačítkem *Vymazat* a narýsovat nový, pokud je s půdorysem spokojený, potvrdí ho tlačítkem *Pokračovat*, tím je půdorys uložen a přechází se na další krok. Během rýsování každé stěny se ve spodní části plátna zobrazuje aktuální délka stěny v metrech.



Obrázek 4.9: Narýsování půdorysu

2) Zakreslení místností

Místnosti se rýsují pomocí jednotlivých úseček. Uživatel si vybere bod na půdoryse nebo na jakékoli již vytvořené stěně a umístí zde počáteční bod nové stěny, ze kterého povede úsečku do koncového bodu stěny. Přidržením klávesy *Shift* může opět rýsovat rovné čáry. Při rýsování stěn se ve spodní části plátna zobrazuje aktuální délka v metrech. Opět lze aktuální krok vymazat a začít rýsovat místnosti od začátku. Pokud jsou místnosti hotové, pokračuje uživatel tlačítkem *Pokračovat* k dalšímu kroku.

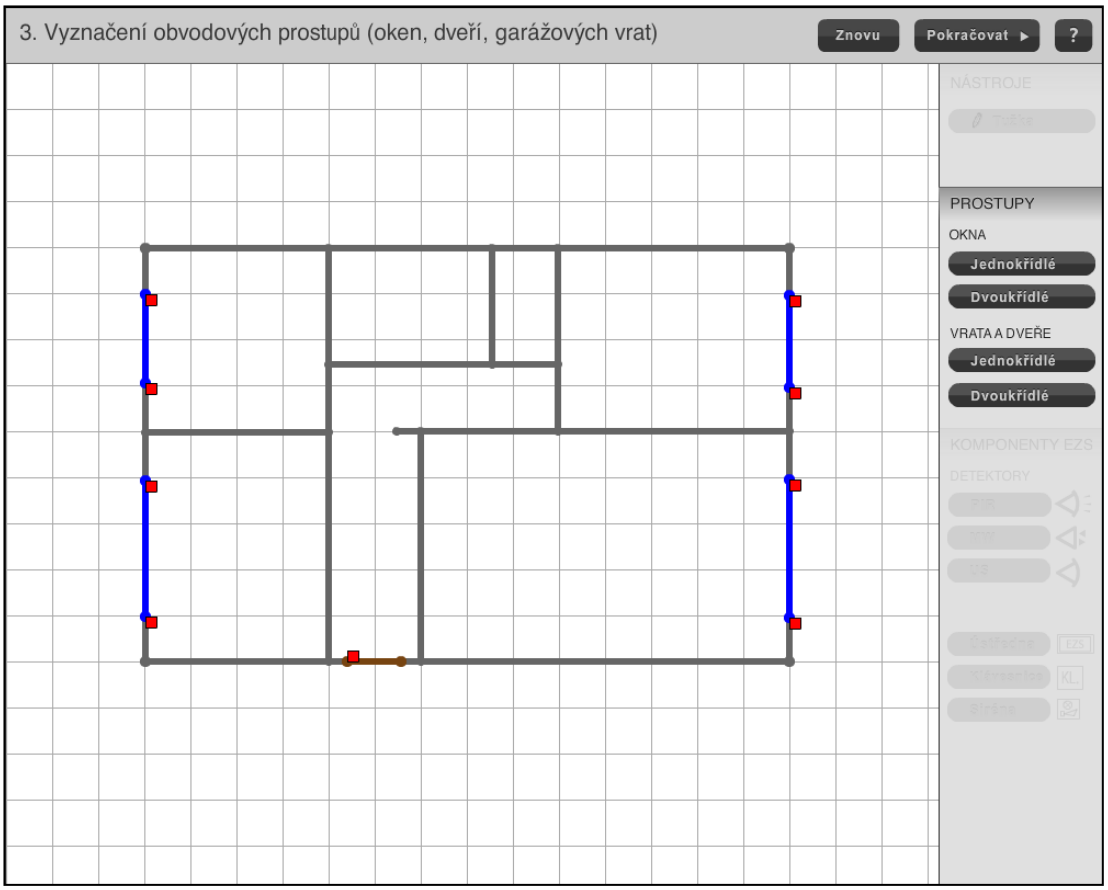


Obrázek 4.10: Zakreslení místností

3) Vyznačení obvodových prostupů

Obvodové prostupy (dveře, garážová vrata a okna) se na perimetru objektu vyznačí zvolením v podmenu, dále vybráním počátečního bodu na stěně obvodu půdorysu objektu a vybráním konečného bodu prostupu na stejné stěně. Prostupy tedy mohou být různě dlouhé, dle potřeby uživatele. Pro zjednodušení bude každému prostupu, po jeho vložení do půdorysu, přiřazena značka magnetického kontaktu v příslušném počtu. Ovšem pouze těm prostupům, které mají být zabezpečeny v závislosti na stupni zabezpečení.

Po vložení všech obvodových prostupů, které je potřebné zabezpečit, je možné aktuální krok uložit tlačítkem *Pokračovat* a přejít k poslednímu kroku návrhu. Pokud se vyznačení nepodařilo, je možné prostupy vymazat tlačítkem *Znovu* a začít nový pokus.

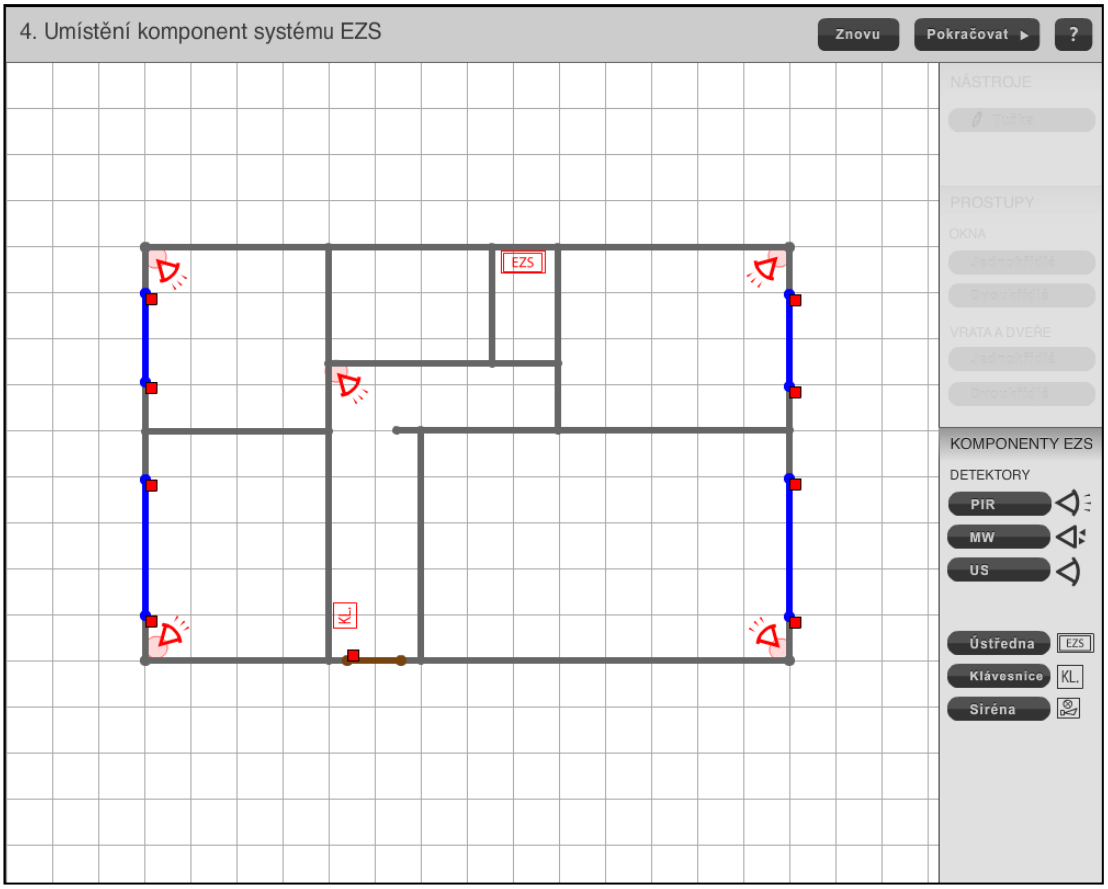


Obrázek 4.11: Vyznačení obvodových prostupů

4) *Umístění komponent EZS systému*

Tento krok vychází z předpokladu, že uživatel je znalý problematiky EZS nebo má již vypracovaný *Textový návrh* a ví, do jaké místnosti vhodně vložit daný typ pohybového čidla. Při každém vybrání konkrétního typu komponentu se uživateli zobrazí nápověda s radami, jak má postupovat při umístění prvku nebo jaké zásady musí umístění splnit. Myšlenkou této práce není vytvořit programové řešení návrhu EZS, které za uživatele udělá celý návrh samo, ale poskytnout uživateli takové informace a rady, na základě kterých se sám dokáže správně rozhodnout, kam daný prvek umístit a proč.

U některých komponent EZS (např. ústředna) není možné bezpečně určit, kam je umístit, aby byly splněny všechny podmínky instalace tak, aby systém mohl bezchybně fungovat. Uživatel sice má možnost tyto prvky do návrhu umístit, avšak tyto mimořádné události bude pro uživatele vhodnější konzultovat s firmami, které se zabývají ukázkovým návrhům EZS.



Obrázek 4.12: Umístění komponent EZS

Grafický návrh si můžete uložit pomocí klávesy PrtScr (Print Screen), vložit do grafického editoru (malování, Gimp, Photoshop aj.) a uložit. Nebo vytisknout či uložit pomocí prohlížeče.

5. ZÁVĚR

Cílem této práce bylo prostudovat a popsat problematiku návrhu elektronických zabezpečovacích systémů EZS a na tomto základě navrhnout vhodnou metodiku návrhu pro objekty stupně zabezpečení 1 a 2. Pro praktické využití navržené metodiky dále realizovat softwarovou podporu, která je založena na webových technologiích. Požaduje se intuitivní grafické a interaktivní rozhraní, které umožní vytvořit kvalitní návrh i laikům.

Pro pochopení problematiky návrhu elektronických zabezpečovacích systémů je nutné se podrobně seznámit s typy jednotlivých komponent EZS, mezi které patří především ústředny, napájecí zdroje, detektory pohybu a vniknutí, signalizační a ovládací zařízení, jejich vlastnostmi, funkcemi a principy fungování. Pro každý prvek EZS totiž platí určitá pravidla instalace a používání, která zajistí spolehlivou činnost celého systému a minimalizuje, nebo eliminuje vznik falešných poplachů. Jediný špatně zvolený prvek může ohrozit spolehlivost a funkčnost celého systému. Dodržování těchto pravidel je v zájmu každého uživatele, který se snaží ochránit svá aktiva. Této problematice je věnována kapitola 2.

Návrh EZS je sled několika důležitých procesů, jejichž cílem je jasně vymezit, jaké negativní faktory negativně ovlivňují objekt, který má být zabezpečen a jaké prvky EZS je potřeba pro spolehlivou funkci EZS v tomto objektu použít. Výsledkem těchto procesů je systémový návrh, který obsahuje osobní údaje o zákazníkovi, informace o zabezpečovaném objektu, stupni zabezpečení, komponentách EZS a třídě prostředí každé z nich, normách a legislativách a další podstatné údaje pro předběžný návrh. Mezi tyto procesy patří: posouzení zabezpečovacích hodnot, bezpečnostní posouzení objektu, zjištění stupně zabezpečení, klasifikace prostředí a volba prvků EZS. Tento návrh je společný pro všechny čtyři stupně zabezpečení. Systémový návrh často slouží také pro orientační zjištění nákladů na zřízení EZS. Tento návrh je podrobně popsán v kapitole 3.1.

Metodika návrhu EZS pro stupně zabezpečení 1 a 2, která vychází z poznatků z obecného návrhu pro všechny stupně zabezpečení, je rovněž sled určitých procesů. Pro první dva stupně zabezpečení bude návrh částečně zjednodušen díky omezené hodnotě aktiv, která mají být zabezpečena, omezeným typům objektů, které mají být zabezpečeny a menšímu výběru vhodných prvků EZS. Navržená metodika tohoto návrhu je podrobně popsána v kapitole 3.2.

Výsledkem práce je webová stránka, která obsahuje teoretické informace o systému EZS, popisuje návrh EZS, vytvořenou metodiku návrhu EZS stupně zabezpečení 1 a 2 a nabízí vytvoření praktického návrhu EZS i pro laiky v textové a grafické podobě. Webová stránka byla vytvořena pomocí redakčního systému Drupal. Textový návrh byl vytvořen za využití programů PHP, Apache a MySQL a správce MySQL.

Požadované grafické intuitivní a interaktivní rozhraní bylo vytvořeno v programu Adobe Flash a naprogramováno v programu Adobe Flex.

Na této stránce se uživatel podrobně seznámí s elektronickým zabezpečovacím systémem EZS a jeho návrhem. Na základě získaných informací si nejdříve vytvoří textový návrh, který mu poskytne informace o počtu, vhodnosti a typu použitelných komponent EZS a přibližné ceně za zřízení EZS pro vlastní objekt. Na základě informací z textového návrhu si uživatel vytvoří grafický návrh EZS vlastního objektu pomocí interaktivní nápovědy. Webová stránka je popsána v kapitole 4.

Webová stránka je přístupná online na adrese *www.ezs.labskalouka.cz*. Tím lze konstatovat, že zadání diplomové práce bylo splněno.

LITERATURA

[1] ČSN EN 50131-1. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. ČNI, Praha 2007. [cit. 2008-12-12].

[2] KŘEČEK, S. a kol.: *Příručka zabezpečovací techniky*. Blatenská tiskárna, Blatná 2003. 350 s. ISBN 80-902938-2-4. [cit. 2008-12-12].

[3] MALÝ, L.: *Návrh metodiky řešení elektronického zabezpečení objektu*. Brno, 2008. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. [cit. 2008-12-12].

[4] PN 50131-1. *Poplachové systémy - Elektrické zabezpečovací systémy - Část 1: Všeobecné požadavky* [online]. [cit. 2008-12-12].
URL: <http://jablotron.cz/upload/File/pn50131-1.pdf>.

[5] PN 50131-1Z1. *Poplachové systémy - Elektrické zabezpečovací systémy - Část 1: Všeobecné požadavky* [online]. [cit. 2008-12-12].
URL: <http://jablotron.cz/upload/File/pn50131-1z1.pdf>.

[6] BURDA, K.: *Zabezpečovací systémy (přednáška 2)* [online]. [cit. 2008-12-12].
URL: < https://www.vutbr.cz/elearning>.

[7] *Drupal* [online]. [cit. 2009-05-01]. URL: <http://www.drupal.cz/ >.

[8] *Adobe* [online]. [cit. 2009-05-01]. URL: < http://www.adobe.com/cz/ >.

SEZNAM POUŽITÝCH ZKRATEK

AIR	- Active Infrared
CCTV	- Closed Circuit Television
DTMF	- Dual-Tone Multi-Frequency
EZS	- Elektronický Zabezpečovací systém
FTP	- File Transfer Protocol
GBS	- Glass Break Sensor
GIF	- Graphics Interchange Format
GSM	- Globální Systém pro Mobilní komunikaci
HTML	- HyperText Markup Language
HTTP	- Hypertext Transfer Protocol
IMAP	- Internet Message Access Protocol
IR	- Infrared
ISP	- Internet Service Provider
JTS	- Jednotná Telefonní Síť
LAN	- Local Area Network
LCD	- Liquid Crystal Display
LED	- Light Emited Diode
MW	- Microwave
MXML	- Minimal eXtensible Markup Language
MySQL	- My Structured Query Language
PC	- Personal Computer
PCO	- Pult Centrální Ochrany
PHP	- PHP: Hypertext Preprocessor
PIR	- Passive Infrared
POP3	- Post Office Protocol version 3
RIA	- Rich Internet Application
SMS	- Short Message Service
SMTP	- Simple Mail Transfer Protocol
SNMP	- Simple Network Management Protocol
SQL	- Structured Query Language
URL	- Uniform Resource Locator
US	- Ultrasonic
WYSIWYG	- What You See Is What You Get
XHTML	- eXtensible HyperText Markup Language
XML	- eXtensible Markup Language

A PŘÍLOHY

A.1 Instalace softwarového řešení návrhu EZS na vlastní PC

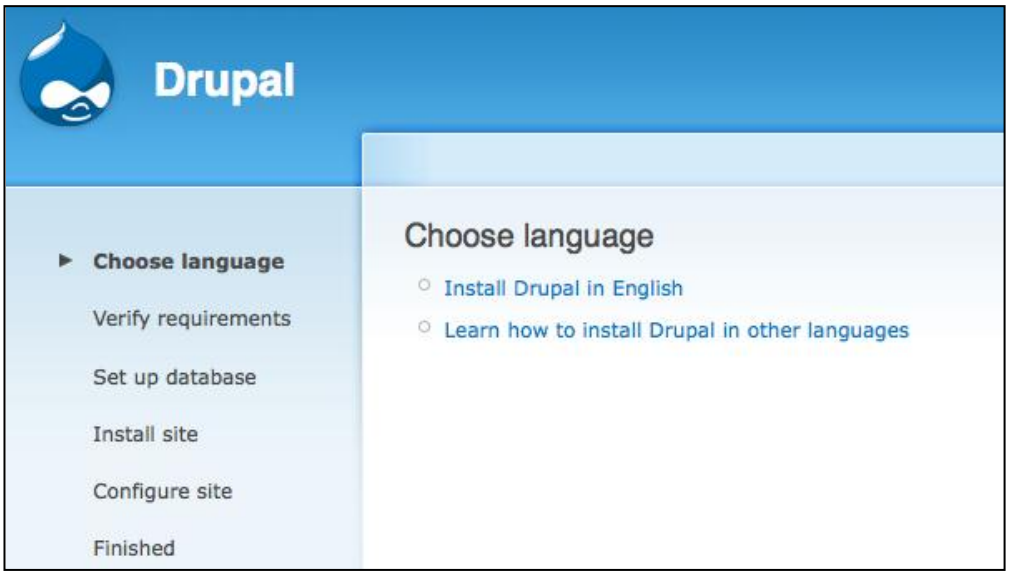
Pro instalaci vytvořeného softwarového řešení návrhu EZS pro stupeň zabezpečení 1 a 2 na vlastní stanici je nutné splnit následující kroky.

1) Instalace PHP, MySQL, Apache, phpMyAdmin
Tyto freewarové aplikace společně slouží k tvorbě webových aplikací. Používáte-li operační systém *Windows*, můžete tyto programy nainstalovat v rámci jediné aplikace. Mezi takové aplikace patří XAMPP, WAMP (Windows Apache MySQL PHP), WampServer, EasyPHP a mnoho dalších. Tato volba se doporučuje začátečníkům pro svou jednoduchost. Další možností je instalace těchto programů samostatně a jejich následovná konfigurace. Pokud se již zabýváte nebo hodláte více zabývat tvorbou webových aplikací, zjistíte, že samostatná instalace všech částí je vhodnější a ve výsledku i přehlednější. Vhodný postup pro individuální instalaci naleznete na adrese *http://myego.cz/item/instalace-apache-mysql-a-php-na-windows*.
V operačním systému *Linux* tyto programy nainstalujete pomocí příslušných instalačních balíčků. Nebo opět v rámci jediné aplikace LAMP (Linux Apache MySQL PHP).
Operační systém *Mac OS X* již webový server Apache a PHP obsahuje v základní konfiguraci. Zbývá tedy doinstalovat databázi MySQL a phpMyAdmin např. podle *http://hivelogic.com/articles/view/installing-mysql-on-mac-os-x*. Pro operační systém *Mac OS X* také existují aplikace, které umožní funkci těchto programů v rámci této aplikace. Mezi takové patří MAMP (Mac Apache MySQL PHP).
Všechny zmíněné programy jsou freewarové (zadarmo) a volně dostupné na internetu.

2) Vytvoření databáze "ezs"
Pomocí programu phpMyAdmin, nebo jeho vhodné alternativy (Sequel Pro, MySQL Administrator) se přihlašte, vytvořte databázi a pojmenujte ji ***ezs***. Nechte ji prázdnou a pokračujte v dalším kroku.

3) Zkopírování složky "ezs" do rootu webu
Z cd přiloženého k diplomové práci si stáhněte soubor ezs.zip a rozbalte jej do rootu (kořenového adresáře) webového serveru (např. /etc/apache2/htdocs, /web/www, /Users/user/Sites).

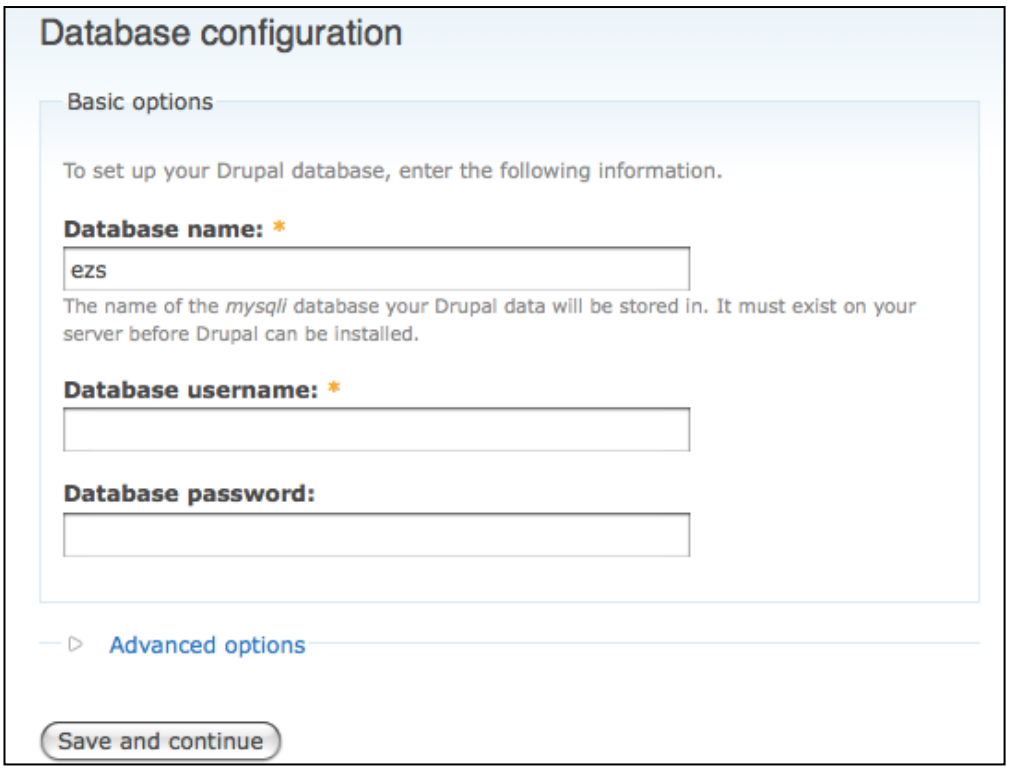
4) Instalace Drupalu
Do prohlížeče nyní napište adresu *localhost/ezs* nebo *127.0.0.1/ezs*, což je odkaz na právě používaný počítač (logická smyčka) a potvrďte. Pokud jste postupovali správně, tak se vám zobrazí následující obrazovka s úvodní obrazovkou **instalace Drupalu**.



Obrázek A.1: Instalace Drupalu

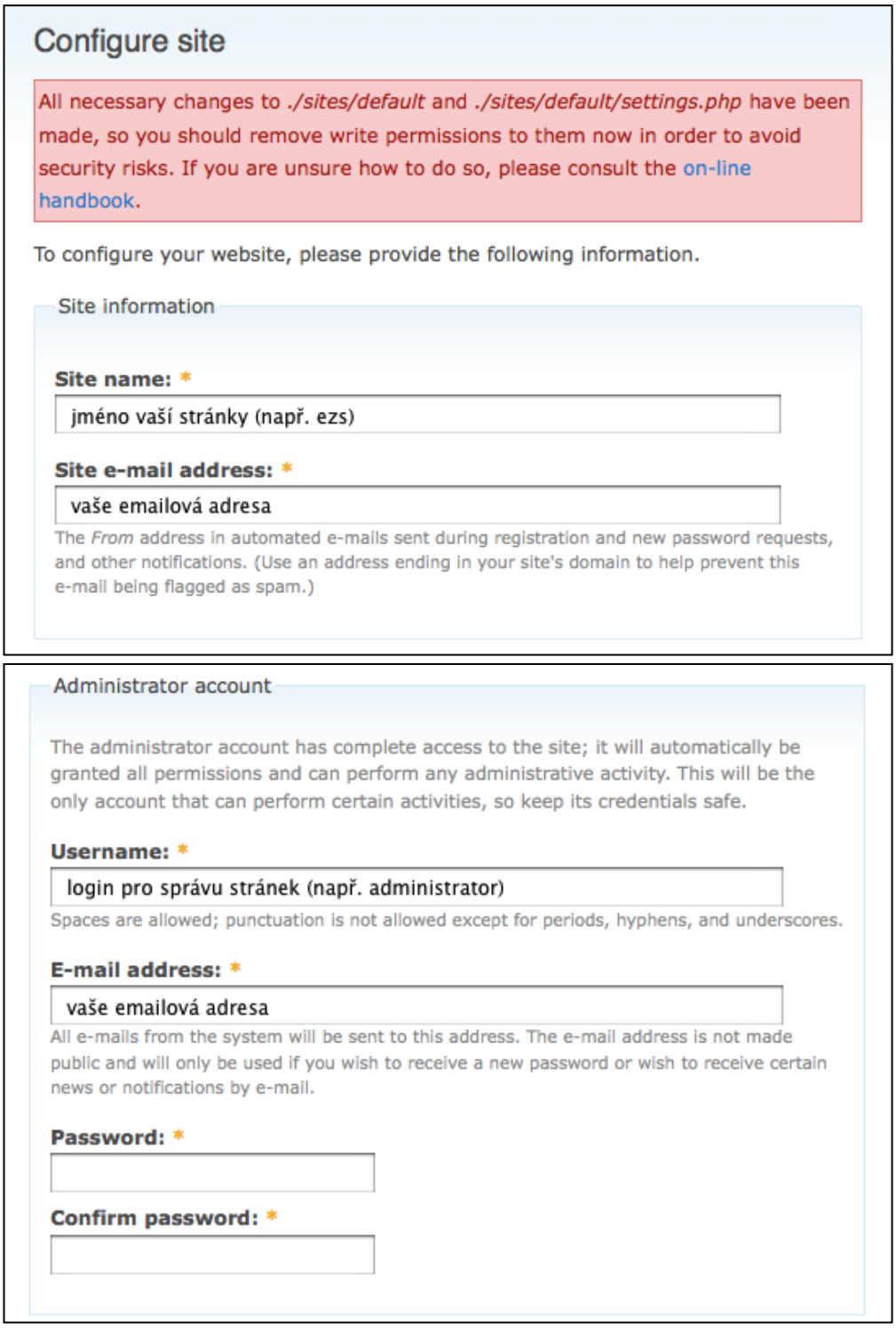
Pokud se vám tato obrazovka nezobrazí, neproběhla instalace některého z programu správně. Postup buď opakujte, nebo zkuste vyřešit zobrazenou chybu sami.

Dále pokračujte na odkaz *Install Drupal in English*. Následuje **konfigurace databáze**. Jméno databáze zadejte *ezs* (toto je nutné v závislosti na vytvořené databázi v kroku 2) dále *login* (přihlašovací jméno) a *heslo* do vaší databáze, defaultně bývá použita kombinace *root* a *password*. Tyto údaje jste zadali při přihlášení do phpMyAdmin. Potvrdíme *Save and continue*.



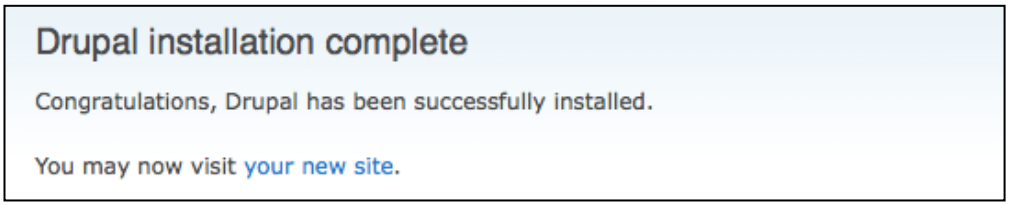
Obrázek A.2: Konfigurace databáze

Dále probíhá **konfigurace stránky**. Vyplňte informace o stránce: *jméno stránky* (např. ezs) a vaši *emailovou adresu* stránky (ta slouží pro emaily o registraci a žádostech o nové heslo, Drupal je redakční systém). Vyplňte informace o administračním účtu: *login*, *emailovou adresu* a *heslo*. S těmito přihlašovacími údaji budete spravovat webovou stránku.



Obrázek A.3: Konfigurace webové stránky

Nastavení serveru nemusíte měnit. Potvrďte *Save and continue*.

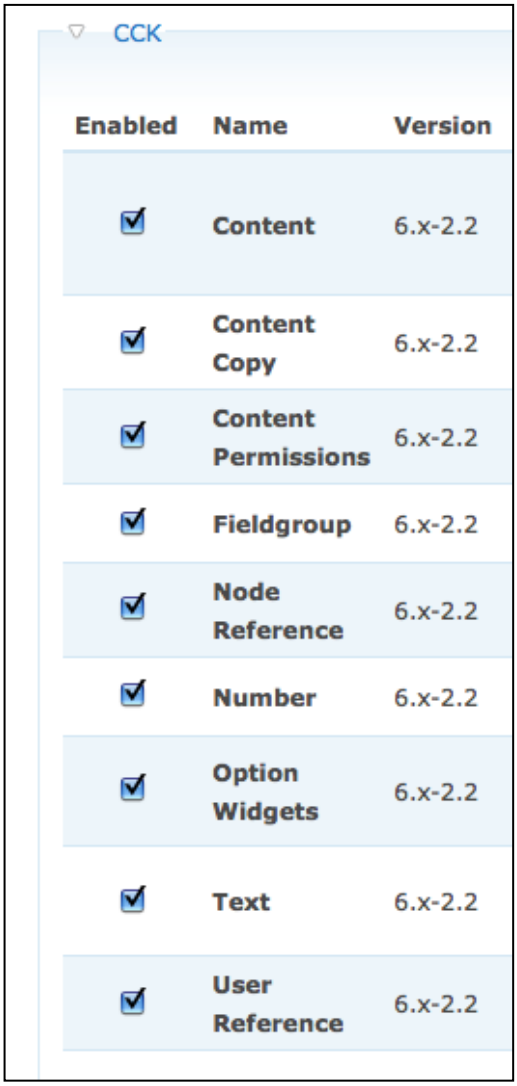


Obrázek A.4: Úspěšná instalace

Instalace Drupalu proběhla v pořádku. Nyní se přihlaste na své stránky z uvedeného odkazu.

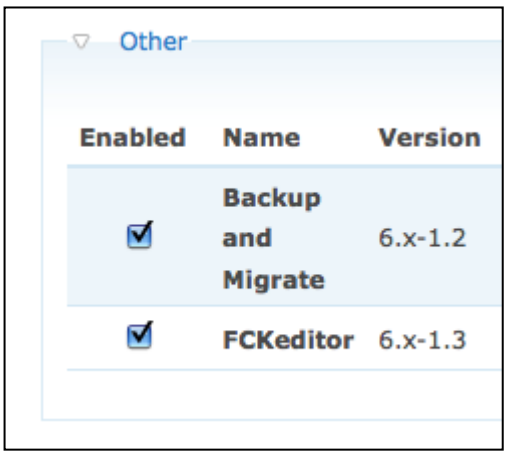
5) Dodatkové konfigurace stránek Drupalu

Nyní přejděte do záložky *Administer* > *Site building* > *Modules* kde povolíte všechny zásuvné moduly v sekci *CCK*.



Obrázek A.5: Zásuvné moduly CCK

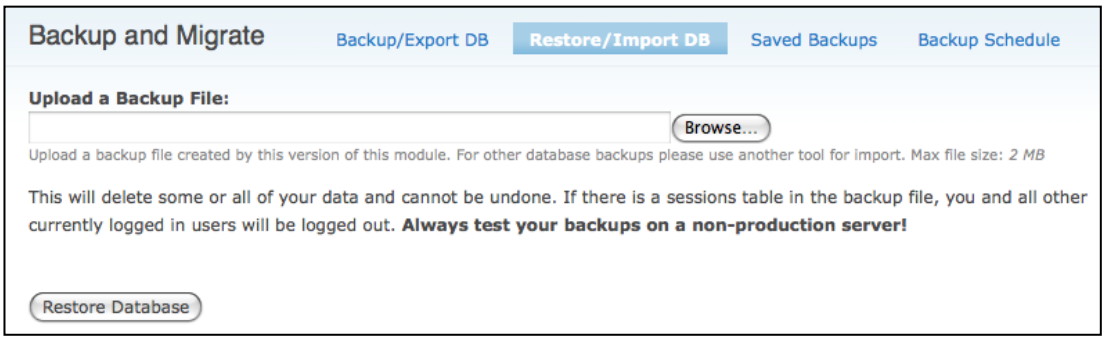
Potvrďte všechny moduly v sekci *Other*. Pomocí modulu *Backup and Migrate* obnovíme zálohu vytvořených stránek v rámci diplomové práce. Modul *FCKeditor* je WYSIWYG editor.



Obrázek A.6: Další zásuvné moduly

6) Obnovení ze zálohy

Nyní jděte do záložky *Administer* > *Content management* > *Backup and Migrate*, zde zvolte *Restore/Import DB*, *Browse...* a vyberte soubor *ezs.sql* ze složky */ezs*.



Obrázek A.7: Obnovení ze zálohy

Potvrďte *Restore Database*.

7) Nastavení připojení k databázi *.php souborů

Nyní otevřete soubor */ezs/designT/conn.php*. Zde vyplňte správné přihlašovací údaje do vaší databáze, stejné jste použili při instalaci Drupalu a při přihlášení do phpMyAdmin. Uložte tento upravený soubor.

Nyní můžete vytvořené stránky se softwarovým řešením pro návrh elektronického zabezpečovacího systému stupně 1 a 2 používat pro vlastní nebo výukové potřeby.